Software Defined Radio Technology for Public Safety

SDRF-06-P-0001-V1.0.0

(Formerly Approved Document SDRF-06-A-0001-V0.00)

Approved
14 April 2006

TABLE OF CONTENTS

Executive Summary 1
1. Introduction 4
1.1. Objective of this Report 4
1.2. The SDR Forum Public Safety Special Interest Group 5
1.3. Methodology 5
2. Overview and Terminology 7
2.1. Overview of the Public Safety Communications Environment 7
2.2. Definitions Relating to SDR Technology 12
2.3. Overview of Military Environment for SDR 14
2.4. Overview of Commercial Environment for SDR 16
3. Benefits/Value to Public Safety of SDR/CR 17
3.1. Interoperability among Public Safety Agencies 17
3.1.1. Areas of Consensus in the RFI Responses 17
3.1.2. Areas of Divergence in the RFI Responses 17
3.1.3. Analysis and Discussion 17
3.1.4. Conclusions 21
3.1.5. Recommendations 21
3.2. System of Systems 21
3.2.1. Areas of Consensus in the RFI Responses 22
3.2.2. Areas of Divergence in the RFI Responses 22
3.2.3. Analysis and Discussion 22
3.2.4. Conclusions 26
3.2.5. Recommendations 27
3.3. Other Users and Commercial Services 27
3.3.1. Areas of Consensus in the RFI Responses 27
3.3.2. Areas of Divergence in the RFI Responses 28
3.3.3. Analysis and Discussion 28
3.3.4. Conclusions 32
3.3.5. Recommendations 33
3.4. Ability to Meet Other Public Safety Requirements 33
3.4.1. Areas of Consensus in the RFI Responses 33
3.4.2. Areas of Divergence in the RFI Responses 33
3.4.3. Analysis and Discussion 33
3.4.4. Conclusions 35
3.4.5. Recommendations 35
4. Considerations for Implementation 36
4.1. Deployment—Infrastructure versus Terminal 36
4.1.1. Areas of Consensus in the RFI Responses 36
4.1.2. Areas of Divergence in the RFI Responses 37
4.1.3. Analysis and Discussion 37
4.1.4. Conclusions 39
4.1.5. Recommendations 40
4.2. Standards 40
4.2.1. Areas of Consensus in the RFI Responses 40
4.2.2. Areas of Divergence in the RFI Responses 40

4.2.3. Analysis and Discussion 41
4.2.4. Conclusions 45
4.2.5. Recommendations 45
4.3. Role of Cognitive Applications 46
4.3.1. Areas of Consensus in the RFI Responses 46
4.3.2. Areas of Divergence in the RFI Responses 47
4.3.3. Analysis and Discussion 47
4.3.4. Conclusions 51
4.3.5. Recommendations 52
4.4. Enabling Technologies 52
4.4.1. Areas of Consensus in the RFI Responses 54
4.4.2. Areas of Divergence in the RFI Responses 55
4.4.3. Analysis and Discussion 55
4.4.4. Conclusions 57
4.4.5. Recommendations 57
4.5. Security 57
4.5.1. Areas of Consensus in the Discussion of RFI Responses 58
4.5.2. Areas of Divergence in the Discussion of RFI Responses 58
4.5.3. Analysis and Discussion 58
4.5.4. Conclusions 65
4.5.5. Recommendations 66
5. Cost Trade-offs, Economic Models, and Business Models 67
5.1. Areas of Consensus in the RFI Responses 67
5.2. Areas of Divergence in the RFI Responses 67
5.3. Analysis and Discussion 68
5.3.1. Cost Trade-off Considerations for Radio Design 68
5.3.2. Life Cycle Costs 72
5.4. Conclusion 78
5.5. Recommendations 78
6. Summary Conclusions, Recommendations, and Next Steps 80
6.1. Conclusions 80
6.2. Recommendations and Next Steps 83
6.2.1. Recommendations 83
6.2.2. Next Steps for the Public Safety SIG 85
6.3. Future Vision 85
A. Acronym Glossary A-1
B. Preliminary Public Safety Business Model B-1
C. Contributors to this Report C-1

LIST OF FIGURES

Figure 3-1 SDR Interoperability Gateway 18
Figure 3-2 System of Systems to Provide Interoperability 23
Figure 3-3 Notional View of System of Systems 25
Figure 3-4 SDR Cost Impact on Options for Expanding Infrastructure 26
Figure 4-1 Infrastructure and Subscriber Examples 38
Figure 5-1 Projected Costs of a Handheld Radio 71
Figure 5-2 Life Cycle Costs 72
Figure B-1 Public Safety Business Model B-1
Figure B-2 Commercial Cellular Business Model B-4

LIST OF TABLES

Table 0-1 Summary of Key Recommendations 3
Table 4-1 Industry Responses for SDR Enabling Technologies 53
Table 4-2 Security Issues in Public Safety Radio 59
Table 5-1 Fixed Cost Comparisons for a Portable Public Safety Radio 69

EXECUTIVE SUMMARY

Public safety communications today are characterized by a patchwork of separate, often incompatible systems with widely varying capabilities in communicating between and amongst systems and user radios. Software defined radio (SDR) capabilities provide a key component of the solution to interoperability as well as increased flexibility and ability to adapt to evolving technologies. These SDR capabilities allow key radio operating parameters to be controlled through software, leading to tremendous flexibility in the radio (e.g., changing frequency bands "on-the-fly" or upgrading capabilities by downloading software over-the-air).

The SDR Forum, through its Public Safety Special Interest Group (SIG), has undertaken this study to assess the potential of and issues associated with SDR technology for the public safety/public protection and disaster response application area. The process by which we have identified and analyzed these issues began with identifying key questions on the topic of SDR technology for public safety. These questions were published in a Request for Information (RFI), to which eight diverse organizations replied. (The RFI and reply comments are included in a separate Annex to this report). The reply comments were then analyzed to identify areas of consensus and divergence among the comments and the Public Safety Special Interest Group.

SDR technology holds the promise of significant benefits to public safety. In fact, some of that promise is being realized today—radio equipment currently being manufactured for public safety use fits most definitions of SDR. The following are key conclusions from this report:

- SDR technology has enormous potential to facilitate seamless interoperability[1] in public safety communications. Interoperability today is limited by incompatible radio systems that operate on different frequency bands and/or use different protocols. Interoperability could best be accomplished through SDR implementation of multi-band radios (e.g., radios that operate on nonadjacent VHF, UHF, and 700/800 MHz bands) and multi-service radios (e.g., public safety land mobile radio, commercial services, and so on) in conjunction with associated modifications to network, infrastructure security, regulatory, and operational procedures.
- SDR also has significant potential for both life cycle cost reduction and enabling cognitive applications that allow a radio to adjust operating parameters automatically to improve performance or better utilize spectrum that enhances performance.
- Technical developments that are needed to realize the above capabilities include front-end processing, analog-to-digital (A/D) and digital-to-analog (D/A) conversion, and portable multi-band antennas. Size, weight, and power consumption constraints of portable units compound these challenges. The technical challenges increase as the range of supported frequency bands increases and as multiple services with significantly differing waveforms (e.g., linear and non-linear) are supported.
- Security is a significant technical issue, with unique security challenges for public safety (see Table 4-2), particularly when reprogramming radios over the air.
- Ultimately there is a role for SDR technology in both the infrastructure and terminal devices, but no preferred sequence of technology introduction was identified.

[1] Interoperability is defined in this report as the ability of public safety emergency responders to share information via voice and data signals on demand, in real time, when needed, and as authorized.

- There is no consensus on the role of standards, in particular the role of the Joint Tactical Radio System (JTRS) Software Communications Architecture (SCA), which is the standard interface used in the military version of SDR. The SCA standard is defined within a device. Public safety land mobile radio standards (such as P25) have historically defined over-the-air interfaces or interfaces between radio system-level components. There is not a standard defined for the interface between components *within* a public safety radio or basestation, however. Thus, adoption of the SCA or a similar interface standard would dramatically change how radios for public safety are developed, procured, and regulated. The issue remains open as to whether such a standard would benefit public safety, and if so, the form that standard might take.
- The economic, business, and cost implications of many of these issues are difficult to quantify at this point because there is a lack of models characterizing these factors that can be used to guide decision-making on research and development (R&D) investment strategies. SDR technology provides new capabilities that can provide value to public safety agencies (e.g., improved interoperability, reduced maintenance logistics). However, better quantification of the total cost of ownership (to include maintenance, training, and upgrade costs) of SDR-based systems is needed to establish appropriate price points for SDR-based public safety communications equipment and systems.

Based on these conclusions, a number of recommendations are made in this report. A more detailed list is included in Section 6.2; key recommendations are listed in Table 0-1.

In addition to these recommendations, based on the conclusions in this report, we identify the following action items and next steps for the Public Safety SIG.

- Develop cost models and business cases to better clarify the cost/benefit trade-offs associated with:
  - Deploying SDR in infrastructure versus terminal equipment;
  - Alternative approaches to meeting public safety requirements with respect to issues, including, but not limited to;
    - Appropriate interfaces for defining standards;
    - The mix of functions and services implemented in a single device;
  - System lifecycle and procurement approaches;
  - Various approaches to deploying SDR, including transition from current systems to multi-band, multi-service capabilities postulated in this report.
- Review updates to the Public Safety Statement of Requirements published by Project SAFECOM and consider a similar review of the Project MESA Statement of Requirements to identify SDR implications.[2]
- Engage standards bodies (e.g., TIA, ETSI, IEEE, OMG, APCO) to jointly consider development of standards related to SDR for public safety.
- Support the SDR Forum's work on cognitive radio definitions.

[2] See references in Section 2.1.

- Engage public safety associations to ensure that they have current information on the progress of the actions and recommendations outlined in this report and to provide information to assist the public safety community in implementing the recommendations for public safety outlined in Table 0-1.
- Work with groups such as the Global Security Architecture Committee and TR-8 to address security requirements and potential solutions.
- Continue providing the venue for public safety users and technology developers to discuss and collectively understand requirements and technology capabilities.

Table 0-1 Summary of Key Recommendations

Recommend that **radio/systems manufacturers** expedite development of:	
	SDR-based multi-protocol, multi-band and/or multi-service radios for public safety applications.
	Diverse waveforms, protocols, infrastructure, networks, and additional technology to support multi-service radios that include land mobile radio and other services relevant to public safety.
Recommend that **components developers**:	
	Expedite front-end and high-speed sampling technology to facilitate practical multi-band radios with wide frequency coverage.
Recommend that **SDR software researchers** investigate:	
	Feasibility of intra-device interface standards (IDIS),[3] including but not limited to those based on the military's Software Communications Architecture (SCA).
	Security technology to mitigate the risk inherent in reconfigurable radios.
	Cognitive applications to enhance interoperability and performance.
	Seamless migration, authentication, and security across systems, as well as support to standards such as P25 ISSI and TETRA ISI.
	Quantitative data on spectrum usage across all services including public safety, commercial services, and other services during major events and incidents.
Recommend that the **public safety community**:	
	Identify and implement operational, training, and procedural changes to take advantage of the capabilities of SDR technology.
	Explore capabilities common to land mobile radios and other services to facilitate multi-service devices and develop a larger market for radio components that can support multiple markets.
Recommend that **regulatory bodies** modify existing regulations to support the capabilities listed above, including:	
	Rules that reflect new models of certification and use of multi-band radios within the existing public safety service as well as multi-service radios (rather than simply modifying rules based on existing models).[4]
	Rules for acceptance and operation of radios if an IDIS is adopted as a standard interface.
	Rules for accommodating evolving cognitive applications.

[3] The concept of an IDIS is described in more detail in Section 4.2
[4] Note that because regulatory regimes differ by country, some rules are already in place to accommodate multi-band and multi-service capabilities discussed in this report.

1. INTRODUCTION

Software defined radio (SDR) technology is rapidly evolving, and is significantly changing the manner in which radio communications capabilities are developed and used in a variety of application areas, such as the military and commercial services. The SDR Forum has undertaken this study to assess the potential of and issues associated with SDR technology for the public safety/public protection and disaster response application area. The purpose of this report is to present key ideas on how SDR technologies can address communications and interoperability requirements for public safety. This report has been prepared by the Public Safety Special Interest Group (SIG) of the SDR Forum to provide information on an issue of significance to both the public safety community and the SDR community. For public safety, SDR holds great potential in addressing challenges such as interoperability and changing radio environments and/or needs. For the SDR community, public safety represents one of the major domains of interest, along with military, commercial services, space/aviation, transportation, and so on. The public safety domain has requirements and a current business base that is somewhere between the specific and highly demanding requirements of the military and the mass-marketing world of commercial services.

1.1. Objective of this Report

This report is intended to serve a number of objectives and a number of different audiences. The first objective is to identify areas of consensus and areas of divergence within the community on aspects of SDR technology for public safety. For example, the report identifies open issues that technical or operational research can clarify; such issues could be referred to other organizations in order to be properly addressed.

Second, for the public safety community and government agencies, this report:

- Identifies the potential value of SDR technology for public safety;
- Identifies cost drivers and key trade-offs;
- Identifies technology gaps;
- Identifies standards; and
- Provides input to a roadmap and projected time frames for deployment of SDR technology.

Third, for manufacturers, this report:

- Identifies standards issues whose resolution could enhance market activity;
- Provides input to the strategic planning and future business case development;
- Identifies critical cost breakpoints; and
- Identifies product improvements and prioritization of features that are important in meeting public safety requirements.

Finally, for the SDR Forum, this report:

- Identifies topics/issues for further analysis by the Public Safety SIG;

- Identifies critical technical issues that can be addressed by working with other working groups within the Forum;
- Identifies critical technical issues that can be addressed by working with groups outside the Forum; and
- Provides input to be used in structuring test, evaluation, and demonstration activities within the SDR Forum.

1.2. The SDR Forum Public Safety Special Interest Group

The SDR Forum is an open, non-profit corporation dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems, with a mission to accelerate the proliferation of SDR technologies in wireless networks to support the needs of civil, commercial, and military market sectors. Activities focus on:

- Developing requirements and/or standards for SDR technologies, including working in liaison with other organizations to ensure that Forum recommendations are easily adapted to existing and evolving wireless systems;
- Cooperatively addressing the global regulatory environment;
- Providing a common ground to codify global developments;
- Serving as an industry meeting place.

The Public Safety Special Interest Group is one of several special interest groups within the Forum that bring together developers, users, regulators, and educators to address issues specific to the application of SDR technology to a particular domain or market area. Goals of the Public Safety SIG are to interface with the public safety community (including both users and vendors), to raise awareness of SDR, to publicize the activities of the Forum in addressing those issues, and to increase participation of the public safety community in the SDR Forum. The Public Safety SIG also interacts with other committees and working groups within the Forum to provide the public safety community's inputs into the publications and initiatives undertaken by the Forum. It is a unique venue, because participation in the Public Safety SIG has historically included public safety organizations, land mobile radio vendors, manufacturers of SDR for military applications, software developers, and regulators.

1.3. Methodology

The Public Safety SIG identified the need for this study in 2004. In order to capture a broad view from the community, the SIG first identified a set of critical questions that addressed various aspects of the value of SDR technology to public safety and published these questions in a *Request for Information* (RFI) in November 2004.[5] The SIG then compiled these results and extracted points of convergence and divergence among the responses for each of the questions. The SIG analyzed the responses and included their own considerations, which are documented in the "Analysis" subsections for each of the topics in Sections 3, 4 and 5. The SIG derived

[5] The RFI was originally published on the SDR Forum's website and is included as an Annex to this report.

conclusions from the RFI responses and the analyses and developed the set of recommendations contained in this report. The discussions that initially led to the RFI and to the development of this report were conducted through regular teleconferences and meetings held in conjunction with the SDR Forum.

2. OVERVIEW AND TERMINOLOGY

2.1. Overview of the Public Safety Communications Environment

Today, public safety[6] communications are characterized by a patchwork of separate, often incompatible systems with widely varying capabilities in communicating between and amongst systems. In the United States, for example, more than 55,000 separate public safety agencies operate communications systems that are based on disparate technologies, frequency bands and protocols. At the same time, there continues to be an increasing demand for public safety agencies to work in concert to react to daily challenges as well as major disasters and events. Interoperability—the ability of public safety first responders[7] to share information via voice and data signals on demand, in real time, when needed, and as authorized—is critical for effective response. Incompatible radio systems can make it difficult or impossible for first responders of different agencies to communicate, making a lack of interoperability a serious problem. Although some public safety groups[8] have achieved interoperability, this is not yet the norm.. Thus, it is common for responders to arrive at an incident with radios that cannot communicate with each other effectively or efficiently. Communications interoperability is a critical issue for day-to-day operations and pre-planned responses, as well as responses to unplanned major incidents. However, it is equally important that communications capabilities be managed, to avoid the chaos inherent in allowing open communication with everyone.

The U.S. Conference of Mayors published a survey of interoperability in June 2004 documenting interoperability challenges facing public safety (see Case Study #1).[9] Current solutions to providing interoperability among disparate systems run the gamut from console patches to cross-band repeaters to audio switches to network-based solutions. Several case studies reflecting these different approaches are included in Case Study #2. These approaches do provide the needed interoperability, but they require additional equipment, and system interconnects and gateways that are not software-based may become obsolete as radio systems are upgraded. Gateway devices require the same transmission to be rebroadcast on additional radio systems, thereby requiring additional system capacity for a single transmission. Deployable repeaters and switches require time to bring them on-site. The goal for public safety is interoperability that is integrated into the radios and systems that they use without specialized equipment, repeated transmissions, and so on. We use the term “seamless” throughout this report to describe this desired level of interoperability.

<text continues on page 10>

[6] We use the term “public safety” in this report, but in the International Telecommunication Union (ITU) and in many parts of the world, the phrase “public protection and disaster relief (PPDR)” is the agreed terminology. For convenience, we have used the term public safety consistently throughout the report, but the acronym “PPDR” could be substituted in all occurrences without changing the meaning of the text or the objectives of the report.

[7] Within this document, the term “first responder” is used to refer to an individual from a police department, fire department, emergency medical team, or other similar organization. His/her responsibilities when responding to an incident are to take necessary action to save lives, protect the welfare of others, and inform other personnel of any potential danger at the scene of an incident. Often the terms “first responder,” “emergency services,” and “public safety” are used interchangeably. These terms generally refer to the same group of people and functions.

[8] For example, public safety agencies in the Washington, DC, metropolitan area in the United States have developed a layered strategy to achieve interoperability through a combination of shared channels, gateways, and radio caches.

[9] Case studies in this report do not reflect the SDR Forum’s endorsement of any specific products cited.

Case Study#1: Interoperability Challenges to U.S. Cities

One of the foremost issues in the [Mayors'] National Action Plan under "Communications and Technology" is the urgent need for interoperable communications across public safety agencies at the local, state, and federal levels. The inability of public safety agencies to be able to talk to one another via radio communication systems, and exchange voice and/or data with one another on demand in real time on a day-to-day basis and during major incidents has been raised by mayors and police chiefs as a continued threat to achieving homeland security.

To help better understand the inability of police, fire, emergency medical service personnel, and other public safety agencies to communicate in real time and in turn advocate for the interoperable needs of cities, the United States Conference of Mayors decided to undertake [a] comprehensive survey.

While the survey findings include encouraging data, including:

- 77 percent of the cities report interoperable capability across police and fire departments and
- 74 percent report that they are interoperable with neighboring city police and fire departments,

the findings also report challenging data.

Many outdated systems are still being used today in cities due to insufficient funds. Older technologies, especially analog systems, lack many of the features that are important to first responders, which are inherent in digital and trunked systems. Older systems may lack the high degree of coverage, security, and information interoperability that is now essential with the war on terrorism. Instantaneous sharing of information, such as video images or fingerprints, is critical to prevent terrorist incidents and to respond to events.

An additional major concern highlighted in the survey refers to the different radio frequencies used by cities. Seventy-five percent of survey cities indicated that different radio frequencies hinder emergency communications between cities.

In addition, 44 percent of the survey cities reported that in the last 12 months there had been an incident or event either within the city or region requiring multi-agency response where the lack of interoperable communications made response difficult.

Among the major city-to-federal findings of important concern is that 58 percent of the cities reported that the current federal mechanism for distributing the majority of homeland security funding through the states has delayed investment in interoperable communications equipment. Other city-to-federal findings of concern include:

- 88 percent reported that they are not interoperable with Homeland Security (FEMA, Customs, Borders…);
- 83 percent reported that they are not interoperable with the Department of Justice (FBI, JTTF, ATF…);
- 75 percent reported that they have not received or been notified that they would be receiving federal funding for interoperable communications.

Among the major city-to-state findings of concern is that 54 percent of the cities reported that the city has not been included as part of the state's interoperability assessment. Other significant city-to-state findings of concern include:

- 60 percent said they are not interoperable with the state emergency operations center;
- 57 percent said that they do not have interoperable capability with the state emergency management agency;
- 49 percent report that their city is not interoperable with the state police.

Among the major city-to-transportation and critical infrastructure findings of concern is that 86 percent of the cities reported that they do not have interoperable capability with the state transportation department. Other significant transportation and critical infrastructure findings of concern include:

- For cities with a major chemical plant, 97 percent reported that they do not have interoperable capability between the chemical plant, police, fire, and emergency medical service (EMS).
- For cities with a major rail facility, 94 percent reported that they do not have interoperable capability between the rail facility, police, fire, and EMS.
- For cities with a seaport, 92 percent of cities reported that they do not have interoperable capability between the seaport, police, fire, and EMS.

Source: Executive Summary of the U.S. Conference of Mayors Interoperability Survey, June, 2004.

Case Study #2A: Inter-System Patches

In Miami, Florida, the Border Patrol, FBI, U.S. Coast Guard, and Monroe County all operate on conventional VHF radio systems in the south Florida region. Miami-Dade County public safety agencies operate on a M/A-COM 800 MHz trunking system, while Broward County operates on a Motorola 800 MHz trunking system. The Florida Department of Law Enforcement (FDLE), Florida Highway Patrol (FHP), and Florida Department of Transportation also operate on a Motorola 800 MHz trunking system. Realizing the need for interoperability, each participating agency established a circuit that connects to the Border Patrol Dispatch Center at Pembroke Pines, Florida. The INS and the FDLE in Miami have a full-time console-to-console link via a leased telephone circuit. The link is used primarily to provide interoperability between INS agents and FHP officers. This interoperability solution has been expanded to include links from INS to the FBI, Metro-Dade County Police Department, Monroe County, Broward County, and the U.S. Coast Guard.

Source: "Local and Regional interoperability Solutions Map," http://www.safecomprogram.gov/SAFECOM/library/technology/1181_localand.htm.

Case Study #2B: Inter-System Patches

The Metropolitan Interoperability Radio System (MIRS) is a system designed to meet the voice communications interoperability needs of the public safety agencies in the Metropolitan Washington (DC) Region. The MIRS is a fixed site system-to-system gateway that features the ACU-1000, an audio baseband switch. The basic system components are interface modules, each of which is designed to connect to 800 MHz, UHF, VHF, low-band VHF radios, along with telephone interconnects. The computer-controlled system is configured to cross-connect up to seven different patches simultaneously. The first MIRS site was established as an operational test bed in Alexandria, Virginia, by the National Institute of Justice. The Alexandria site was originally configured to cross-connect the Alexandria Police Department's 800 MHz radio system, the Metropolitan Police Department's UHF system, and the U.S. Park Police's VHF system. Subsequent system expansion led to capabilities to link any of twenty-one agencies in the region, and sites similar to Alexandria were established in other parts of the National Capital Region.

Source: National Institute of Justice, "Metropolitan Interoperability Radio System - Alexandria Site Description Document," CommTech Report No. TE-02-03.4 April 2003.

Case Study #2C: A Network-based Interoperability Solution

The 1999 Columbine High School shooting incident was a horrific event for the people of Colorado, and an astounding challenge for the first responders who attempted to deal with it. The combination of multiple agencies and incompatible radio systems at the scene severely hampered their responses.

Mindful of this problem, and faced by communications issues at subsequent multiple responder situations since Columbine, the Denver Police Department (DPD) has been seeking an interoperability solution. After a field trial held in Denver in December 2004, the DPD selected M/A-COM's NetworkFirst to solve its interoperability problem once and for all.

"We've kept the NetworkFirst demo running since we set it up last December," says Dana Hansen, the DPD's superintendent of communications. "It's worked just fine the entire time, helping local police, fire, and EMS communicate freely with each other plus the FBI, DEA, and the US Marshal."……

Connected to all the participating agencies, the Network Switching Center plays telephone operator; automatically routing traffic to and from each agency's voice gateway (which converts the transmissions from IP to voice and vice versa) as required. The result is instant interoperability; one that can easily accommodate network players simply by deploying more voice gateways and connections to the Network Switching Center…..

Thirteen incompatible radios systems run by local, state, and federal agencies were patched into a NetworkFirst Switching Center established for the trial. As well, the city's police, fire, and EMS agencies remapped their radio channels to make room for three NetworkFirst talk groups.

These were designed to be provisioned by the NetworkFirst Switching Center; ensuring that each and every portable radio in the area now had true interoperable communications. The benefits were immediate; allowing state troopers using Motorola radios to talk to DPD officers on M/A-COM portables….

Source: "Denver Picks Network First," by James Careless, from Law and Order Magazine, Aug 2005.

Case Study #2D: A Network-based Interoperability Solution

Florida Gov. Jeb Bush announced plans for a statewide wireless communications system.

The new contract through the State Technology Office will allow local law enforcement and first responders to communicate with any other jurisdiction using their existing radio systems and frequencies. Florida is the first state to use the Motobridge IP solution on a statewide level, according to Motorola.

"Through the network, dispatch centers will have unprecedented capabilities to communicate with each other to coordinate response and radio users will be able to talk directly to all other users," said Simone Marstiller, Florida's chief information officer, at the announcement in Jacksonville.

Some switch systems are going into place nationwide as short-term radio interoperability solutions, because jurisdictions are using proprietary systems and cannot communicate across systems. Motobridge is an Internet protocol gateway switch, which means that it is able to include more management of frequencies and identification features, according to Motorola.

The Motobridge equipment will go to more than 200 local dispatch centers in Florida's 67 counties. Because it is a state contract, it will be able to use the state's intranet and other statewide resources, Florida officials said.

Source: "Florida to Build Wireless System," by Diane Frank, from Federal Computer Week, December 10, 2004.

Public safety communications faces other challenges as well. Spectrum (radio frequencies) is limited, especially considering that technological advances provide a wealth of information, thereby increasing the demand for spectrum. Spectrum for voice communications is a challenge because the mission-critical nature of public safety means that the network must be available for immediate communications transmissions at all times. Examples of information capabilities include downloading security video to a police car, monitoring firefighter biometrics and equipment status, and providing real-time access to hazardous material information. These new types of information must be transmitted to the right place at the right time. Another challenge involves the logistics required to upgrade several hundred or several thousand radios by physically bringing them to a radio shop to be reprogrammed. Upgrading to new technology is also a challenge, especially if the technology is not backward compatible with existing radios and/or infrastructures. Leveraging commercial hardware and software development, improving ease of use, and reducing life cycle costs are also seen as beneficial to the public safety community but are challenging to achieve. Costs and affordability have traditionally been a limiting factor in what the public safety community has been able to deploy.

Future public safety communications will likely be deployed in (or addressed by) a system of systems, which rely on a variety of existing and new networks, standards, protocols and frequency bands. They must support environments ranging from short-range communications, such as personal area networks (PANs), to long-range communications at a national or international level.

Several ongoing efforts are currently focused on the communications needs of public safety personnel and agencies, including the following:

- CommTech

  The U.S. Department of Justice's National Institute of Justice (NIJ) CommTech Program has a mission to assist state and local law enforcement agencies to effectively and efficiently communicate with one another across agency and jurisdictional boundaries. It is dedicated to studying interoperability options and making valuable information available to law enforcement, firefighters, and emergency technicians in different jurisdictions in communities across the country.

More information about NIJ's CommTech Program can be found at: http://www.ojp.usdoj.gov/nij/topics/commtech/.

- Project SAFECOM

  The flagship program for public safety communications in the United States is Project SAFECOM, managed by the U.S. Department of Homeland Security. SAFECOM's mission is to serve as the umbrella program within the federal government to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications. One of the first items developed under Project SAFECOM was a comprehensive analysis of public safety communications requirements. The results of this analysis were documented in a *Statement of Requirements*, which is available at: www.safecomprogram.gov.

- Interoperable Communications Technology Assistance Program (ICTAP)

  ICTAP is a technical assistance program designed to enhance interoperable communications among local, state, and federal emergency responders and public safety officials. ICTAP is associated with the Department of Homeland Security's Urban Areas Security Initiative (UASI) grant program. The goal of the ICTAP program is to enable local public safety agencies to communicate as they prevent or respond to a weapons of mass destruction (WMD) attack. ICTAP also leverages and works with other federal, state, and local interoperability efforts whenever possible to enhance the overall capacity for agencies and individuals to communicate with one another. More information on the ICTAP program can be found at: http://www.ojp.usdoj.gov/odp/ta_ictap.htm.

- Project 25

  P25 is an ongoing activity under the auspices of the Telecommunications Industry Association (TIA) for the wireless industry to develop and maintain public safety standards for digital equipment and systems that will assist the life-saving and damage-control activities of first responders at the scene of an emergency or disaster situation. Information on P25 can be found at: www.tiaonline.org/standards/technology/project_25/.

- Project MESA

  The Public Safety Partnership Project (PSPP), Project MESA (Mobility Emergency Safety Applications), is a collaborative recommendation effort between the European Telecommunications Standardisation Institute (ETSI) and TIA for the next generation of high mobility wireless data standards. These new standards are envisioned to cover the transfer of digital voice, data, video and infrared video, and other digital data applications at high data rates between and among MESA user devices and external network components. Project MESA's activities are intended, among other objectives, to support the efforts of the member countries in meeting their own public safety and public service wireless data telecommunications requirements. The *Project MESA Statement of Requirements* is available at www.projectmesa.org.

- TErrestrial Trunked RAdio

  TErrestrial Trunked RAdio (TETRA) is an open digital trunked radio standard defined by ETSI to meet the needs of the most demanding professional mobile radio users. The TETRA Memorandum of Understanding (MoU) was established in December 1994 to create a forum which could act on behalf of all interested parties, representing users, manufacturers, application providers, integrators, operators, test houses, and telecom agencies. Today, the TETRA MoU represents more than 100 organizations from all continents of the world. More information on the TETRA MoU is available at www.tetramou.com.

2.2. Definitions Relating to SDR Technology

There are several definitions for software defined radio. The SDR Forum defines software defined radio as:

> a collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and user terminals. SDR provides an efficient and comparatively inexpensive solution to the problem of building multi-mode, multi-band, multi-functional wireless devices that can be enhanced using software upgrades. As such, SDR can really be considered an enabling technology that is applicable across a wide range of areas within the wireless industry.
>
> SDR-enabled devices (e.g., handhelds) and equipment (e.g., wireless network infrastructure) can be dynamically programmed in software to reconfigure the characteristics of equipment. In other words, the same piece of 'hardware' can be modified to perform different functions at different times. This allows manufacturers to concentrate development efforts on a common hardware platform. Similarly, it permits network operators to differentiate their service offerings without having to support a myriad of handhelds. Finally, SDR provides the user with a single piece of scalable hardware that is at once compatible at a global scale and robust enough to deliver a 'pay as you go' feature set.[10]

The SDR Forum also notes that reconfigurability can be "achieved through the use of a set of clearly defined APIs[11] residing on top of a flexible hardware layer."[12]

Note that SDR does not refer to a single device, technology, or level of capability. In fact, several levels have been described by the SDR Forum to help illustrate the levels of capability that might be implemented in communications devices:

- Tier 0—Hardware Radio: The radio is implemented using hardware components only and cannot be modified except through physical intervention.
- Tier 1—Software Controlled Radio: Only the control functions of a Software controlled radio are implemented in software. Thus, only limited functions are

[10] From the SDR Forum's Website (www.sdrforum.org) in the Frequently Asked Questions (FAQs) under "About SDRF."
[11] API is the acronym for Application Programming Interface.
[12] From the SDR Forum's Website (www.sdrforum.org) in the Frequently Asked Questions (FAQs) under "About SDRF."

changeable using software. Typically, this extends to inter-connects, power levels, etc., but not to frequency bands and/or modulation types.

- Tier 2—Software Defined Radio: Software defined radios provide software control of a variety of modulation techniques, wide-band or narrow-band operation, communications security functions (such as hopping) and waveform requirements of current and evolving standards over a broad frequency range. The frequency bands covered may still be constrained at the front-end, requiring a switch in the antenna system.
- Tier 3—Ideal Software Radio: Programmability extends to the entire system (e.g., with analog conversion only at the antenna, speaker and microphones).
- Tier 4—Ultimate Software Radio: Ultimate software radios are defined for comparison purposes only. They accept fully programmable traffic and control information and support a broad range of frequencies, air interfaces, and applications software. The radios can switch from one air interface format to another in milliseconds, use GPS to track users' locations, store money using smartcard technology or provide video so that users can watch a local broadcast station or receive a satellite transmission.

In addition to the definitions provided by the SDR Forum, adopted definitions and activities with definitions under development will be of interest to public safety and readers of this report. The FCC has adopted the following definition for its regulatory purposes:

> *Software defined radio:* A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.[13]

Note that the sole purpose of this regulatory definition is to specify the set of devices that are subject to initial FCC certification, testing, and special security rules. SDRs that meet this definition are eligible for the advantageous streamlined FCC approval of subsequent software changes.[14] There is also substantial work under way in the ITU on this topic, including definitions of SDR, software controlled radio, reconfigurable radio, and policy-based radio. Hence, it is important to be aware of the evolving nature of relevant terminology.

Throughout this report we also use the terms multi-protocol, multi-band, and multi-service, defined as follows:

- **Multi-protocol** refers to operations within public safety land mobile radio but using different protocols such as P25, conventional FM, and the manufacturer's proprietary protocols.

[13] Federal Communications Commission, First Report and Order, ET Docket No. 00-47 (FCC 01-264), September 14, 2001.

[14] Note that this certification may very well be in addition to, but not a replacement for, FCC part-specific certification. For example, a Part-90 SDR will likely have to meet both SDR criteria and specific operational criteria for Part-90 operation. In this case, the SDR criteria is simply how the Part 90 requirements are implemented.

- **Multi-band** refers to operations in more than one frequency band (e.g. VHF, UHF and 800 MHz). As noted in Section 2.1, public safety radios are licensed in several different frequency bands. Multi-band radios refer to radios that can operate in more than one of these bands. Multi-band can refer to both adjacent band radios (e.g. 700 MHz/800 MHz radios) and multi-octave radios (e.g. VHF/UHF/800 MHz). Adjacent band radios are also available; however, the technical challenges of multi-band radios described in the remainder of this report refer to non-adjacent multi-band radios.
- **Multi-service** refers to radios that can operate across multiple services (public safety land mobile radio, Wi-Fi®, WiMAX, cellular). Generally, the services also operate in different frequency bands as well. (Note that this use of the term "services" does not refer to police services, fire services, emergency services, and so on.)

2.3. Overview of Military Environment for SDR

The U.S. Department of Defense has been faced with challenges analogous to public safety in terms of implementing communications among incompatible radio systems. In fact, the proliferation of incompatible and "stovepiped" communications capabilities within the military motivated much of the early work in SDRs in the mid-1990s. This rationale for the initial application of SDR technology is reflected in Case Study #3. Based on successful proof of concept, the Department of Defense embarked on a major program to transition all tactical communications capabilities to SDR technology under a program known as the Joint Tactical Radio System (JTRS).

JTRS is a standardized, integrated approach to wireless communications via radio. Interoperability rests on the capacity of JTRS to communicate with existing (legacy) tactical communications systems in the near term as well as to provide integrated information to support joint military operations in the long term. JTRS is intended to achieve interoperability by:

- Adhering to a common Software Communications Architecture (SCA);
- Using common software applications waveforms;
- Utilizing standard security procedures and algorithms; and
- Undergoing thorough testing and certification.

JTRS will provide simultaneous, real-time access to multiple channels of information, including maps, visual data, sensor data, and voice communication. Protocol conversion and message format translation will allow bridging between systems with dissimilar protocols. JTRS will also provide the ability to retransmit information on different frequency bands/waveforms to facility interoperability with non-interoperable legacy networks. Other features include:

- Multiple simultaneous full- and/or half-duplex channels;
- Digital waveform emulation to allow simultaneous translation among multiple radio frequency (RF) systems and networks; and

- Ability to bridge between terrestrial RF, fiber-optic, cable, and/or wire systems and airborne or space-based communications systems.[15]

Note also that "JTRS is also working with the North Atlantic Treaty Organization (NATO) Consultation, Command and Control (NC3) Board Communications Network Subcommittee and its ad hoc Radio Working Groups to develop new NATO standards (STANAGs) to support future software defined radios."[16]

Case Study #3: SDR for Interoperability and Waveform Portability

by LTC (Ret) David M. Fiedler

Ever since the United States (horse) Cavalry developed a requirement in the early 1920s for a battery-powered radio that could be operated and held with one hand while on a moving horse, the Army has loved the idea of handheld radio communications. Through the decades the hand-held radio idea has been developed and refined with some notable successes such as the vacuum tube and crystal technology SCR-536 walkie-talkie of World War II and the AN/PRC-6 handy-talkie of the Korean War era.

The lesson here is that all ground tactical units including combat support and combat service support units rely each other and on aircraft in operations and need to communicate across all force components securely to be effective! The idea that parts of a force can use unique radios and operate in a communications vacuum just doesn't work or make sense.

By the late 1990s into this tactical communications jumble stepped the U.S. Special Operations Command whose communicators woke up and saw the value of handheld tactical radio communications that could operate across all frequency bands, modulation modes, and waveforms being used in the DoD. SOCOM had long rejected the "big" Army's requirements and material development process so they went forward to develop a handheld radio using their own requirements and procurement methods. The result of this effort was the development of a new and unique handheld radio named the AN/PRC-148 or Multiband Inter/Intra Team Radio. MBITR went into full production in FY-2000.

The AN/PRC-148 is currently used throughout the U.S. Department of Defense and also by other allied governments. The radio was developed by U.S. Special Operations Command primarily to reduce the physical signal equipment load on the individual SOF soldier while at the same time enhancing mission communications interoperability capabilities. Prior to the development of the AN/PRC-148 individual SOF unit S-6s tailored to their mission requirements a huge variety of existing tactical radios all operating on small portions of the 30-512MHz frequency spectrum that all used different waveforms and modulation schemes. What the AN/PRC-148 provides in a single package is a highly flexible tactical communications solution useful over a very broad range of combat environments. As a small example, before the AN/PRC-148 many units man-packed separate AN/PRC-119s (SINCGARS) for ground-to-ground communications (30-88MHz), and AN/PRC-113s for ground-to-air communications (115150 & 225-400MHz) on each mission. This way of operating was complicated and prone to cause operational mission failures when only a single radio malfunctioned because each operated in different frequency bands. The AN/PRC-148 successfully solved the multiple radio problem using one secure, light weight, high performance, handheld package that could be issued redundantly and thus serve as its own backup radio. In addition due to its reduced size, weight, and power consumption characteristics, many additional radios could be carried if needed without increasing the space, weight, and power budget for the mission.

The article was originally published in Army Communicator, Summer 2005, Vol. 30 No.3 a U.S. Army Publication approved for public release, distribution unlimited. Mr. Fiedler is a retired Signal Corps lieutenant colonel and retired senior Department of the Army electronics engineer. His last assignment as a DA Civilian was Project Director Commercial Tactical Radios, a part of the Office of the Project Manager for Tactical Radio Communications Systems (PM-TRCS), Fort Monmouth, N.J.

[15] *JTRS Brochure*, available at http://jtrs.army.mil/documents/jtrs%2Bbrochure.pdf.
[16] http://jtrs.army.mil/sections/overview/fset_overview.html?overview_international.

In addition to JTRS, the Department of Defense has been transforming their communications to a broad system of systems, a net-centric capability known as the Global Information Grid (GIG). The GIG will incorporate communications devices developed under the JTRS program. The GIG is designed to link information system elements into a "system of systems" to provide smooth and timely flow of information to whomever needs it.

2.4. Overview of Commercial Environment for SDR

In addition to the development of SDR technology to meet military applications, there is ongoing work in commercial applications. For example, SDR technology is currently being deployed by Mid-Tex Cellular in their basestations, using software developed by Vanu, Inc. Mid-Tex Cellular is overlaying its existing TDMA-based wireless network with a new GSM/GPRS-based system by installing a radio access network (RAN) composed of HP servers and Vanu software. The software based solution is key for Mid-Tex Cellular, as they are a small service provider that relies substantially on a large percentage of roaming customers. They must support a large number of protocols relative to their customer base and be able to cost-effectively upgrade as protocols change.

In terms of research and development, one of the most significant projects currently under way is the End-to-End Reconfigurability (E2R) project sponsored by the European Commission. The objective of the effort is to "devise, develop, trial and showcase architectural design of reconfigurable devices and supporting system functions to offer an extensive set of operational choices to the users, application and service providers, operators, and regulators in the context of heterogeneous systems."[17] The technology developed under this program is intended to facilitate the deployment of capabilities that allow users to seamlessly access voice and data from a variety of heterogeneous networks. Although the research is focused on commercial applications, many of the same challenges—the ability to dynamically reconfigure to access different networks, efficient spectrum utilization, lower field maintenance and upgrade costs, devices/platforms that can accommodate multiple services, and increased flexibility that can benefit users and operators—are long-term goals for public safety communications as well.

[17] http://phase2.e2r.motlabs.com/project_overview.

3. BENEFITS/VALUE TO PUBLIC SAFETY OF SDR/CR

3.1. Interoperability among Public Safety Agencies

SDR technology can help to improve interoperability among public safety agencies by providing the ability to tie together these disparate systems or provide flexible capabilities that facilitate radio access to disparate systems. The RFI asked respondents to discuss how SDR could facilitate interoperability.

3.1.1. Areas of Consensus in the RFI Responses

- All reply comments agreed that SDR could help provide a technical solution capable of operating in multiple frequency bands and utilizing multiple transmission modes to connect various public safety radio systems. M/A-COM, Motorola, and Thales mentioned that they already ship Tier 2 SDR equipment that can handle multiple waveforms.
- SDR could help enable remote over-the-air radio upgrades.
- Although most wireless products manufactured today are software-based, the advantages of SDR are less evident as radio bandwidths and data rates increase. This fact is especially true for handheld devices.
- JTRS and the Ad Hoc Working Group stated that SDR technology could also be used as an interoperability bridge between two systems.
- M/A-COM noted the importance of management and regulatory issues to interoperability. Without management and regulatory policies in place, the full technological benefits of SDR will not be realized.

3.1.2. Areas of Divergence in the RFI Responses

- The JTRS Program emphasized the importance of intra-device radio standards to interoperability. This issue is addressed in more detail in Section 4.2.

3.1.3. Analysis and Discussion

While the full capability of SDR has yet to mature, the implementation of certain aspects of SDR technology has already been deployed within the public safety sector. Thales Communications notes that “an example of a current product with this type of capability is the AN/PRC-148…that covers 30-512 MHz in a single SDR portable radio” and supports multiple protocols of FM, AM SINCGARS, ANDVT and HAVEQUICK I and II. M/A-COM identified the “new P7200 portable and M7200 mobile radios [that] support OpenSky™, EDACS™, PROVOICE™, P25, and analog-FM protocols, features, and networks …, with a common hardware platform.” Motorola noted that the “XTS and XTL series of portable and mobile radios that support analog FM protocols, Securenet™, and the P25 conventional and trunked protocols using one platform, which are available in the VHF, UHF, or 700/800 MHz Public

Safety bands." These examples highlight the evolution of multi-band and multi-mode radios that can provide increased public safety interoperability.

SDR technology can also be used as an interoperability bridge between two systems. JTRS replied that "[because] most of the new SDRs will have multi-channel capabilities, they will also be capable of performing as wireless gateways at incident sites. These gateways will translate voice and data communications between various agencies' legacy equipment that were formerly incompatible." **Error! Reference source not found.** provides a pictorial representation of how the gateway could operate. The Ad Hoc Working Group envisions a switch that could appeal to both the commercial and public safety markets. An "SDR-equipped unit, such as a van, can be used on site to bridge between existing radios that can not otherwise talk with each other."

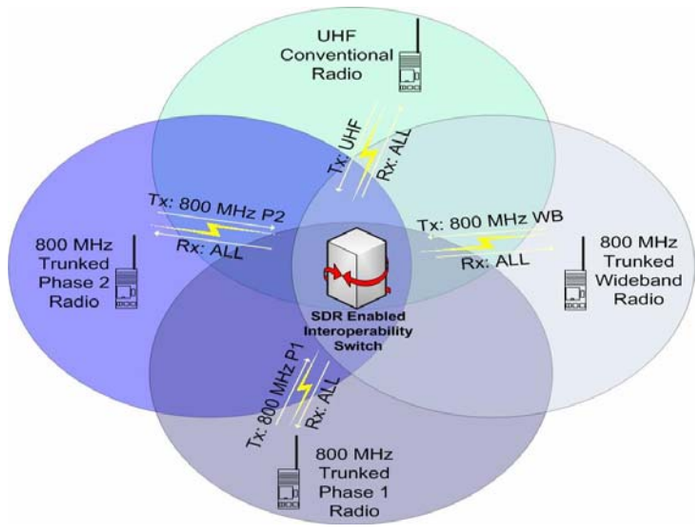

Figure 3-1
SDR Interoperability Gateway

The Public Safety SIG also noted that SDR can enhance the functionality impacted by software downloads, which may improve public safety interoperability. Over-the-air software downloads provide the ability to dynamically update a radio's characteristics. This capability improves interoperability by further enabling radios to be reconfigured to meet the requirements of the incident to which the subscriber is responding. This seamless interoperability with minimal user intervention is a model that could be achieved as multi-band, multi-service SDRs become well-established in the public safety community.

Motorola noted that "the benefits provided by SDR are greatest for narrowband, low data rate systems. The SDR benefits diminish as radio bandwidths and data rates increase." This comment primarily referred to the added benefit of SDR in typical land mobile radio (LMR) systems versus using SDR for broadband systems such as 802.11-based systems, which operate under one or more established standards in the 802 series. High-bandwidth, high-speed data devices that can operate on several of the 802 variations are generally available today at relatively low cost due in part to the high volume of the consumer market, whereas narrowband, low data rate devices generally incorporate only a few of the protocols that are operated in that environment and are typically more expensive. Therefore, the benefits of SDR technology are greatest in the narrowband low data rate environment. However, this could change as non-802.11 protocols are implemented.

Tier 2 SDR radios, capable of multiple protocols and both 25 kHz (often referred to as wideband) and 12.5 kHz (often referred to as narrowband) operation, are already demonstrating SDR technology applications to address interoperability. For example, as public safety agencies in the United States are mandated to transition to 12.5 kHz operations, interoperability with

legacy systems operating on 25 kHz channels can be maintained by deploying Tier 2 SDR radios that operate on both protocols/waveforms. Consider the situation of two agencies that have compatible radio systems. The agencies program channels from each other's system into their radios to support mutual aid and interoperability. If one municipality were to upgrade their radio system to a system technology that was not backward compatible with the other system, it would not be able to communicate with hardware-only radios. However, if the upgrading agency purchased Tier 2 SDR radios with multiple waveforms, the technology would support the same method of "cross programming channels." In this manner, existing SDR radios help ensure that interoperability is maintained as public safety agencies upgrade their communication systems.

The benefits of SDR technology will not be realized without dealing with several issues, including equipment cost, bandwidth requirements, and regulatory hurdles that may limit the ability of SDR to improve interoperability. M/A-COM replied that barriers other than the technology itself existed, such as "funding, operational policies, institutional barriers" and cooperation among public safety agencies. As an example, "the radios' users must be licensed to operate on all relevant bands in whatever geographical area interoperability operations are going to be conducted." The Ad Hoc Working Group also commented that "the situation rapidly becomes more complex as the number of organizations involved increases." M/A-COM added their concern from a security aspect because the "deployment of SDR for interoperability has raised new attention from the FCC regarding techniques for SDR device certification and concern that unauthorized emissions could result if an unauthorized person were to 'hack' into the radio code through software downloads or other means."

SDR technology must also be matched by organizational support. As SDR radios become more sophisticated, the number of features they provide can grow tremendously. Features intended to greatly enhance interoperability often come with a number of operational issues that must be addressed. These issues include authentication, training in the use and maintenance of this new technology, and updated Tactical Interoperable Communications Plans (TICP) and policies that reflect the flexibility of SDR technology.

For example, when first responders arrive at an incident scene, they must be able to connect to a radio network to communicate. If the first responders are using a digital trunked radio network, this requires that the radio network be able to interact with the radios. Note that currently there are public safety communications systems that utilize proprietary protocols. SDR technology could facilitate development of radios that include multiple proprietary waveforms from different vendor systems, which would provide even greater interoperability options than multi-band radios that support only non-proprietary protocols. However, development of such a radio requires the manufacturers of the proprietary systems to license the intellectual property associated with the proprietary protocols. In the absence of such agreements, interoperability is limited to standardized interfaces (e.g., P25) and conventional, non-proprietary protocols (such as those implemented on national interoperability channels in the United States).

Interoperability also requires that all parties use an agreed-upon authentication system. For interaction and authentication to properly take place, the proper training needs to have occurred and the correct policies need to have been implemented. These types of issues will need to be addressed before the full benefits of SDR technology to public safety interoperability can be realized.

In summary, SDR technology can improve public safety communications interoperability by enabling communications across disparate systems. The technology must be complemented by management, operational, and regulatory solutions. Like many other technologies, SDR could be a major factor to improve communications, but the implementation is expected to be evolutionary in nature.

Although not specifically referenced in the responses to question #1 of the RFI, responses to other questions and subsequent analyses of the RFI responses within the Public Safety SIG revealed other significant advantages to public safety in deployment of SDR technology beyond interoperability. In order to highlight these as part of the value to public safety, these potential benefits are listed in this section as well:

- **Reduction of costs associated with upgrading/modifying equipment** — Changing the configuration of a radio, whether to upgrade software to a new version or reprogram the channels on a radio, can be a costly and time-consuming operation for an agency responsible for thousands of subscriber radios. Often, each radio must be physically transported to a radio shop, which makes reprogramming a logistical and configuration management challenge. Over-the-air software downloads have the potential to significantly simplify this entire process. More discussion on the impact of SDR technology on costs is included in Section 5.
- **Ability to adapt to evolving technologies and standards** — SDR technology can significantly facilitate the introduction of new technologies and evolving standards to the field by simplifying the process required to take advantage of technologies or become compliant with new standards. The flexibility of SDRs provides opportunities to "future-proof" systems, that is, to significantly facilitate the cost and complexity of migrating systems to accommodate new capabilities, standards, technologies, and so forth.
- **Ease of operation** — SDR technology can be used to hide "implementation details" from users to provide more seamless radio operation to end users. For example, a user need only know that channel 5 is the city fire department tactical channel; the user need not be concerned whether that channel is operating at a VHF, UHF, 700 or 800 MHz frequency or whether his/her radio is compatible with the fire department system.
- **Performance optimization** — The role of cognitive applications is addressed in more detail in Section 4.3, but we note in this section that the flexibility inherent in SDR technology, coupled with cognitive capabilities, provides the basis for powerful tools to enhance the performance of radio systems. Capabilities to adjust the parameters of the waveform as required to most efficiently interface with the rest of the system, given varying atmospheric, interference, and other conditions, could significantly improve the quality of radio system performance, especially under adverse conditions. One specific aspect of this concept involves SDR/cognitive capabilities to utilize spectrum in a more efficient manner (spectrum efficiency through dynamic spectrum allocation).

3.1.4. Conclusions

- SDR technology has significant potential to enhance communications capabilities for public safety. There are several different scenarios in which interoperability could be significantly improved with the deployment of SDRs that incorporate multiple waveforms (e.g., multiple frequency bands, multiple channel widths and configurations, and multiple protocols).
- While interoperability is the most compelling argument for SDR technology, several other significant potential advantages of SDR technology include the potential of cost reduction for upgrading and maintaining equipment, the ability to adapt to evolving technologies and standards, ease of operation, and performance optimization.
- Manufacturers are implementing certain aspects of SDR technology in available public safety communications products.
- Full realization of the benefits of SDR technology for public safety requires organizational and procedural changes within public safety agencies to match the capabilities made available by the evolving technology.
- To fully exploit SDR technology, regulatory changes will be required that accommodate new models of certification and use rather than modifying rules to current models. Note that because regulatory regimes differ by country, some rules are already in place to accommodate the multi-band and multi-service capabilities discussed in this report.

3.1.5. Recommendations

- Investments by both government research programs and manufacturers to develop and deploy SDR technology should continue, specifically resulting in multi-protocol, multi-band, and/or multi-service radios for public safety applications.
- Public safety agencies should begin considering operational, training, and procedural changes to effectively take advantage of the capabilities of SDR technology, particularly in enabling new or more effective communications options for first responders. The Public Safety SIG should work with public safety to help determine technology implications and develop materials to assist in the dissemination of the information to public safety users.

3.2. System of Systems

The future of public safety radio communications can best be described as a “system of systems,” or a large number of individual radio systems that must be interconnected to support first responder’s mission-critical communications needs. The system of systems concept could be realized through incorporation of SDR technology into the networks, standards, and protocols that would enable short- and long-distance communications in multiple frequency bands and interoperability among components. The RFI asked for comments on SDR support for the system of systems concept as well as the limitations of SDR to support this capability.

3.2.1. Areas of Consensus in the RFI Responses

- Four reply comments stated that SDR technology will facilitate the development of a single terminal device, thereby minimizing hardware variations, tying together multiple legacy and domain-specific transmission requirements and providing for multi-protocol, multi-band, and multi-service capabilities to enhance interoperability.
- The issue of network control and management was raised in most reply comments, particularly when dealing with security concerns, operational procedures, spectrum efficiency, and intersystem roaming. While comments pointed out that SDR technology would solve the problem of connecting multiple, disparate systems, security requirements and resource command and control were specifically noted as key aspects of network and infrastructure management that will influence the successful integration of SDR technology into existing systems.
- All parties recognized the benefit of SDR technology to facilitate interoperability, but some noted that because network infrastructure is a vital part of interoperability SDR technology alone cannot compensate for inadequate infrastructure.

3.2.2. Areas of Divergence in the RFI Responses

- One of the reply comments noted that the inherent economics of software, which is characterized by a significant up-front development cost followed by very low marginal distribution costs. As the number of devices sold increases, the overall unit cost (total cost divided by the number of copies sold) declines because of the lower recurring and distribution costs, resulting in potential benefits for consumers of these devices. However, subsequent discussion within the Public Safety SIG identified a variety of factors that can influence the cost of software-based products.

3.2.3. Analysis and Discussion

Five of the reply comments recognized the benefit of SDR to facilitate the growth of the system of systems concept, and another comment noted that SDR will improve a radio's "versatility of usages." Two of the reply comments noted that control and management were the bottlenecks of the technology development.

The advancement of SDR technology should lead to the development of user terminals and other infrastructure that will seamlessly connect (and disconnect) on demand using disparate, individual radio systems. The Ad Hoc Working Group replied that "SDR technology is important for reducing the number of hardware variations required," which effectively makes the system of system concept vendor-agnostic, assuming that any proprietary vendor licensing can be resolved. Thales Communications noted that user terminals "can adapt to whatever connectivity is available in a given area." This allows incident responders to communicate on any existing infrastructure within range. The flexibility greatly improves interoperability among on-scene responders as well as off-scene command and control.

SDR technology can be used to interconnect the system of systems landscape, thus improving the transfer of voice, data, and video among radios that are based upon various

protocols and frequency ranges—a situation that often occurs during a multi-discipline incident response. There are several approaches to implementing SDR to support the system of system concept. Infrastructure-based SDR, where the basestation dynamically adapts to the transmitting radio's configuration, enables legacy systems of all types to communicate when the subscriber units are within range of the SDR basestation. Alternatively, terminal equipment can reconfigure to accommodate the system with which it needs to operate at any given time. A simple concept of subscriber equipment reconfiguration in the system of systems concept is shown in Figure 3-2. Consider an EMS provider who normally operates with a UHF P25 Phase 1 conventional system. When called to assist in a neighboring jurisdiction, the radio would be reconfigured to operate on an 800 MHz Trunked Phase 2 system. Upon arrival at the incident, the radio would then reconfigure to operate on a 4.9 GHz incident network.

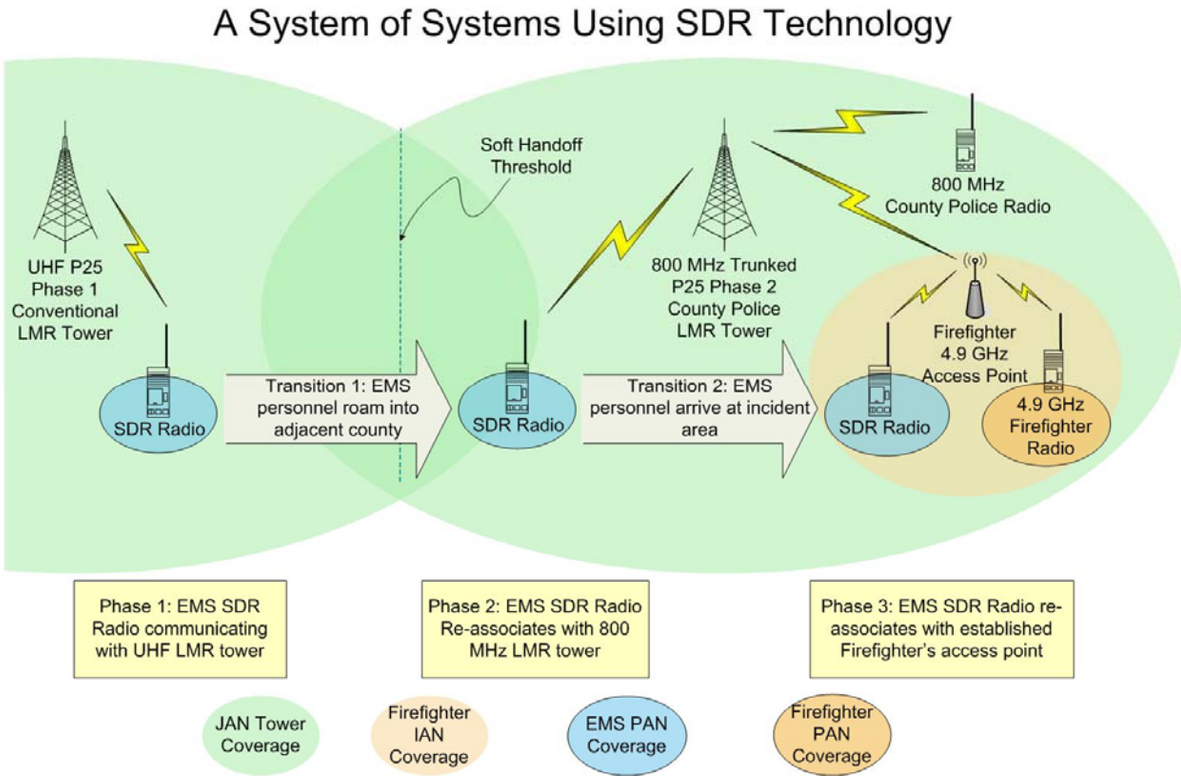

Figure 3-2
System of Systems to Provide Interoperability

Due to the sheer number and differences between individual systems, network control and management issues must be accounted for when employing SDR technology under the system of systems construct, particularly as technology moves to more sophisticated digital capabilities. M/A-COM emphasized in their response that "a multimode [multi-protocol] radio could support roaming between two disparate systems as long as site adjacency information was relayed between the two systems, and the radio was authenticated on both systems, and encryption information was shared." M/A-COM added that the SDR radios should "support digital voice connectivity between disparate systems with the capability of transcoding... [and] transcripting" information between two systems. The relay of information shared between systems would still have to follow regulations and guidelines set forth by affected public safety agencies. Motorola

replied that "roaming should be consistent with operational procedures established by the public safety chiefs or commanders of the involved systems." Information shared among radios as described above should remain transparent to the user, dispatcher, and system administrator. "The radio user would most likely want features to look and feel the same no matter what 'system' they happen to be connected to," noted M/A-COM. These issues must be addressed to ensure the adoption of SDR technology into the system of systems construct.

SDR technology in support of the system of systems concept is complementary to the ongoing P25 standards activities under the purview of the TIA Committee TR8. Specifically, the Inter-RF Subsystem Interface (ISSI) standard addresses non air-interface protocols when roaming between land mobile radio systems. The ISSI will ultimately support the transfer of authentication information and handoff conversations to allow a user to roam seamlessly from one network to another. But the ISSI will not by itself provide interoperability between radios operating in different frequency bands, and it is focused specifically on the interface between land mobile radio systems. As the ISSI standard is completed and adopted, SDR technology provides additional capability that can facilitate compatibility between P25 compliant and legacy systems and provide multi-band and multi-service radios that incorporate P25 waveforms in addition to other capabilities. More discussion of standards for public safety SDR is contained in Section 4.2.

The system of systems concept can be extended beyond the traditional LMR systems to include a variety of communications capabilities that complement LMR. SDR technology provides a means to develop devices that allow seamless use of multiple systems as dictated by the requirements of the communications and the availability the transport mechanism. A notional view of such an environment, incorporating traditional LMR and evolving technologies, is shown in Figure 3-3. It illustrates the concept of multiple systems using multiple protocols, technologies, and standards that have a many-to-many mapping to different levels of networks.

Another key consideration within the systems of systems model is the set of cost trade-offs associated with the development of one device that incorporates a large number of modes and features versus multiple devices that incorporate a small number of modes. The public safety community has identified the need to carry and maintain various devices currently in use as a challenge to efficient communications, and has indicated a desire to see SDR technology development result in reducing the number of communications devices required to access the variety of communications capabilities typically used by public safety personnel. The manufacturers noted potential disadvantages of incorporating increasing numbers of features and modes into a device, including the following:

- Increased development time;
- Features and modes that are not used by a majority of users can drive up the cost of the device without providing overall value; and
- Interactions among simultaneously executing feature sets in a radio increases the complexity of the system, requiring more extensive testing to ensure reliability.

Although SDR technology significantly facilitates the creation of devices that can be reconfigured to meet functional requirements, it does not eliminate the need for careful consideration of the trade-off between the number of features supported in a particular device

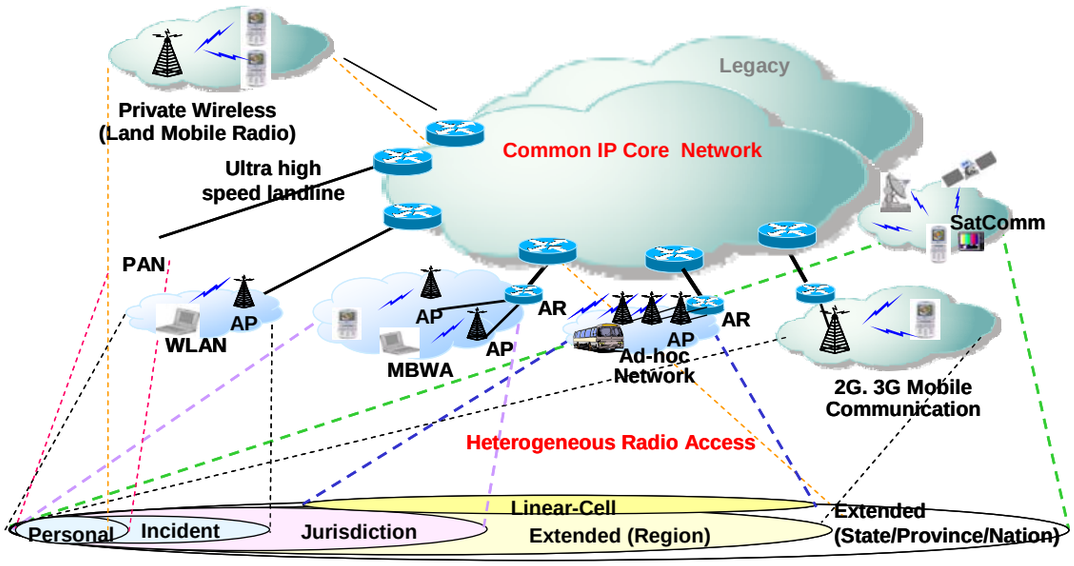

Figure 3-3
Notional View of System of Systems

and product cost and time to develop that device. These trade-offs differ significantly between portable radios and mobile radios due to the size, weight, and power constraints of portable radios. It should also be noted that, historically, the technologies to support multiple modes within a radio have evolved as new features and are phased into a device at a measured pace. Paragraph 5.3.1 provides additional discussion of trade-offs between the number of features supported and product cost.

With respect to the system of systems concept, the proliferation of commercial standards-based, large-bandwidth, high-throughput technologies available in the marketplace (such as Wi-Fi and WiMAX) have given public safety agencies greater choice for improving their communications capabilities. One of the attractive aspects of this technology is that the costs are low due to the current mass market base for such devices. Initial SDR-based technology may have a higher initial cost when compared to these other technologies. However, widespread adoption into the public safety community will lead to economies of scale and make SDR more cost effective over the long term. A system of systems concept can be used to reduce system maintenance costs and to extend the life expectancy of legacy systems. An example of this concept is shown as a system expansion in Figure 3-4. Currently, in many major metropolitan areas, available frequencies are scarce. If a public safety agency needs to acquire additional frequencies, they may be forced to build an entirely new system in a different band (Option 1). However, using SDR technology, the agency could simply build out the new channels in a different band (Option 2) and use SDR multi-band radios to allow users to communicate in the appropriate band. By eliminating the need to completely replace the original system, Option 2 provides a great cost savings (e.g., Option 2 will require 20 fewer transmitters, less maintenance, etc.) in this example.

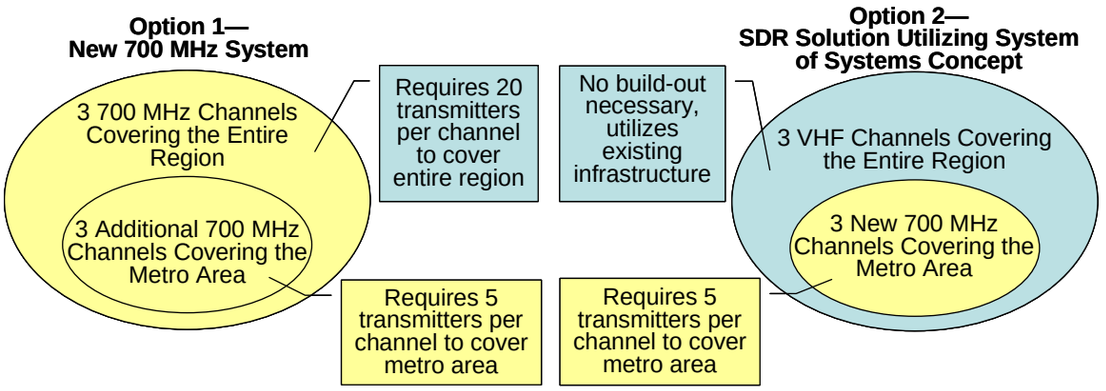

Figure 3-4
SDR Cost Impact on Options for Expanding Infrastructure

SDR technology may ultimately enable a seamless single-device solution that will allow public safety agencies to coordinate response efforts quickly and efficiently. While most Public Safety SIG members thought that subscriber-based SDR would be a more effective solution for the development of a system of systems, the consensus was that infrastructure-based SDR would be less expensive and simpler. Reply comments also agreed that several issues, such as operations, network management, governance, and proprietary protocols, must be further examined before SDR can be fully utilized in the system of systems.

As a final observation on the notion of systems of systems, we note that the military is transforming their communications to a broad system of systems, net-centric capability known as the Global Information Grid. The GIG will incorporate communications devices developed under the JTRS program. Although the GIG is intended to address requirements much broader than those of public safety communications, as technology is proved out in the GIG and it matures, applications to public safety should be considered.

3.2.4. Conclusions

- The flexibility inherent in SDR technology facilitates multi-protocol, multi-band and multi-service devices that can operate across multiple systems, thereby supporting the "system of systems" concept for public safety communications.
- Several key technical issues must be addressed to allow seamless migration across systems, including relaying of site adjacency information across disparate systems, authentication, and sharing of encrypted information. Operational procedures must also be put in place to ensure smooth operation in a system of systems environment.
- Care must be taken in the design of a single-device solution to avoid creating devices that become unwieldy and overly expensive in an attempt to accommodate dissimilar functional requirements.

3.2.5. Recommendations

- Research should be conducted to more explicitly define how SDR technology can support the implementation and adoption of the P25 ISSI and how the ISSI might eventually be enhanced to support and exploit SDR capabilities.
- Research should be conducted on SDR support of seamless migration across systems, authentication across systems, and handling of encrypted information across systems.
- The Public Safety SIG should continue to monitor developments in the military's GIG program (see Section 2.3) and E2R (see Section 2.4).

3.3. Other Users and Commercial Services

Sections 3.1 and 3.2 look at the issue of how SDR can impact the ability of public safety first responders to communicate among themselves, both in terms of traditional land mobile radio systems and in the "system of system" architectures envisioned for the future. This section considers how SDR can facilitate the communication of first responders to non-first responders, including the perspective of the use of non-public safety communications capabilities. Specifically, the RFI asked for responses to the following questions:

- How can SDR technology facilitate interoperability between public safety radio systems and other domains (e.g., transportation, telematics, utilities, etc.)?
- How can SDR technology facilitate multi-modal devices that provide the user access to land mobile radio networks, commercial cellular system, paging systems and wireless data systems?
- Which other domains have overlapping requirements that could expand the size of the market base?
- What complications (e.g., technical, operational and/or regulatory) arise when interfacing to commercial, private, public, and military domains?
- What are the practical limitations of SDR technology in implementing such capabilities?

3.3.1. Areas of Consensus in the RFI Responses

- SDR functionality has the potential to enable radios that can function across a wide range of air interfaces. That capability could permit interoperation between services that are currently unable to talk with each other, provided that management, infrastructure, regulatory and network support is in place and the RF performance of the other service's air interface (bandwidth, TX linearity, etc.) is compatible with the public safety radio.
- Due to limitations of size, weight, and power, adding enough SDR capability to handheld units to enable such operation is very difficult.

- Public safety could benefit from some aspects of military radios, such as functionality, operational capability, reliability, and security. Similarly, public safety could benefit from the economies of scale that characterize commercial units. Conversely, the extent to which public safety radios have unique requirements may result in the disadvantages of low production volumes, challenges to adapt quickly to new technology, higher cost, and potentially less functionality.

3.3.2. Areas of Divergence in the RFI Responses

- The responses disagreed about the ability to get meaningful SDR functionality across a useful range of services.
- The responses disagreed about whether multi-use "one-size-fits-all" systems are practical, given the wide variation in form factor, screen capability, keyboards, frequencies, bandwidths, transmission (TX) linearity requirements, and user interfaces in existing equipment.
- The responses disagreed about the extent to which commercial service network providers will be willing to adapt their systems to the requirements of the public safety market and whether there is a business case.
- The responses disagreed about whether providing most of the adaptation in the infrastructure is meaningful, or whether handsets have to be very capable in order to see viable benefits. (Note: This issue is addressed in Section 4.1).
- The responses disagreed about whether the benefits of open standards, which inherently carry added overhead burdens, are justifiable over leaner and limited proprietary approaches (see Section 4.2 for discussion of standards issues).
- The responses disagreed about whether the public service community will adapt to new modes of operation in order to take advantage of efficiencies provided by the use of other services, or whether they will insist on imposing current operating procedures on any system they adopt.

3.3.3. Analysis and Discussion

The discussion in Sections 3.1 and 3.2 focus on the potential impact of SDR technology on the ability of first responders to interoperate with other first responders and interface with public safety–focused communications systems. But first responders will need to communicate outside their own communications systems to effectively respond to incidents as well as to perform their daily functions. For example, amateur radio services have been used in disaster response for many years. In addition, a number of new radio options have become available for public safety use, both licensed and unlicensed. Among them are cellular/PCS, Wi-Fi, WiMAX, Bluetooth® and ultra wide band (UWB). In addition, Citizens' Band (CB) and Family Radio Service (FRS) services have been used for public safety applications. These services all have different characteristics, capabilities, functionality, and economic models. Depending on the situation, some may benefit the public safety community, and some will not. As viable product offerings,

such as the cellular telephone, have become commonly available at low cost, public safety organizations have made use of them.

3.3.3.1 Issues in Multi-Service Applications

Use of these new communications options presents rapidly increasing logistics and cost problems; for example, different services currently require different hardware devices. This section explores the capabilities of services that appear to offer prospects for future functional enhancement and lower life-cycle cost and analyzes the role for SDR technology in promoting utilization of these expanded capabilities.

Interoperability with users outside the public safety domain has additional technical (radio and network/infrastructure), management, and regulatory implications. Not only must radio interaction be provided, but differing operating procedures must be resolved. For direct communication with other licensed domains, licensing schemes will have to adjust to make the variable operations legal prior to implementation. Institutional barriers and dissimilarity of operations policies between public safety and other domains must be addressed

Network considerations become more difficult as well when attempts are made to operate seamlessly with networks of other domains. One problem is the difficulty of translating the public safety features (such as a talk group or an emergency declaration) onto another type of network. Also, the network would need to address security or grade of service on commercial networks.

Technically speaking, software programming a public safety radio to operate with new air interfaces and features of other domains (for authorized operation) is achievable provided that:

- The new mode's bandwidth and dynamic range requirements do not exceed those requirements existing in the radio to be reprogrammed.
- The radio transmitter (especially the power amp) has sufficient linearity if the modulation happens to be one that requires such linearity.[18]
- There is sufficient reserve capacity in the radio's processors and memory to accommodate the new mode and its features.
- The radio's switching speed will support any TDMA modes that might be added.
- The radio's filtering and stability is sufficient to meet transmit (TX) spectrum requirements and receive (RX) adjacent channel rejection requirements.

Design margin, relative to the above factors, can be built into the radio to enable economies of scale by using the same hardware for other air interfaces as well as simplifying air interface upgrades. The amount of margin that is allocated in the radio design is a delicate balancing act in the design trade-off process. Certainly, the size, weight, and power consumption, due to the added design margin, must not be excessive relative to public safety's stringent requirements, and the added cost of the design margin must not outweigh the economies of scale cost savings.

[18] Traditional modulations that have been used for public safety are "constant envelope" and do not require a linear amplifier.

3.3.3.2 Service-Specific Considerations

Some of the technical factors for incorporating additional air interfaces into a radio for interoperating with various specific services are considered here.

Transportation, Utilities, Paging

The modulations and features for interoperating with transportation, utilities and paging do not represent a major technical impact on the design of the public safety radio. The operating bands and bandwidths are similar, and the feature requirements are less stringent than for public safety, so there will be minimal processor impact. Incorporating the air interface for these users into a public safety radio is not difficult from a technical standpoint, and, in fact, variations of existing public safety radio products are often used today by both utilities and transportation services.

Wi-Fi, WiMAX

Compared to typical public safety radios that are designed to operate on 25 kHz channels, Wi-Fi and WiMAX are data-intensive, operate on much higher frequency bands (2.4 GHz and above), and utilize channels with bandwidths that are orders of magnitude greater than public safety voice radio channels. Also, modulations for these modes require linear transmitters as opposed to the transmitters typically used for constant envelope modulations in public safety radios. Constant envelope transmitters can achieve much higher power levels (typically 3 watts or greater for even a portable) at lower cost than if linearity is also required. As such, cost/performance trades suggest that a single device including waveforms to support both public safety air interfaces (designed to stringent performance specifications and higher power) and a Wi-Fi and/or WiMAX waveform would most effectively be implemented as a supplemental Wi-Fi/WiMAX module to the radio (a "black-box" device). Such an approach would leverage existing and emerging commercial off-the-shelf (COTS) modules and chipsets to affect these air interfaces, but would not fit the definition of an SDR.

Cellular Services

Many cellular standards in existence today span bandwidth requirements ranging from being comparable to typical 25 kHz public safety channels to much higher for 3G+ data-intensive services. For reasons that are discussed further in Section 4.4, the services that operate near the public safety 800 MHz band would be easier and less costly to include in an 800 MHz public safety radio than those that are an octave away in frequency, such as PCS-1900. However, today's higher-speed cellular services tend to utilize modulations that require linear transmitters, whereas the typical public safety radio does not require linearity. As with the air interfaces in the previous paragraph, implementing a linear transmitter in a public safety portable radio that can also meet public safety's comparatively higher power requirement (typically 3 watts or greater) is a technical challenge and cost driver.

Mesh Networks

For many years, mesh technology has been implemented and proven effective in wired networks as a form of information distribution for many years. Recently, the public safety arena has started to use mesh networks as both a more reliable wireless local area network (WLAN) and for first responders to exchange critical real-time information where infrastructure does not already exist. The TIA TR-8.8 Subcommittee is investigating the use of mesh network technology as a wireless broadband standard in the 4.9 GHz band, possibly in combination with

either an IEEE 802.11 or 802.16 based standard. The challenges facing the development of standardized mesh technology include frequency coordination, power management, and dynamic routing paths, each of which influences another, further complicating the issue.

Bluetooth

Bluetooth uses low power transmissions to provide short-range coverage. Due to the 9.14-meter (30-foot) range of Bluetooth, it has been used primarily as a personal area network (PAN) to replace wires or optical links connecting nearby devices. For instance, public safety could use Bluetooth in a wireless lapel microphone for a portable radio. However, because Bluetooth operates in the 2.4 GHz unlicensed band, it has the same interference concerns as Wi-Fi. These concerns—the limited coverage range and newer technologies such as UWB—have limited the adoption of Bluetooth by the public safety community. The technical issues associated with development of SDRs that accommodate linear waveforms as well as public safety waveforms described with respect to Wi-Fi® and cellular systems also apply to Bluetooth.

Ultra Wide Band

UWB is another emerging technology that may provide numerous public safety applications. Applications include imaging systems and asset tracking in addition to other applications currently provided via Wi-Fi and Bluetooth. UWB is still in the standards development phase, which is the leading challenge facing UWB development. Currently, multiple (and incompatible) approaches to UWB standardization are being advocated by different industry groups. In addition, work is ongoing to ensure that UWB does not create harmful interference that degrades the performance of other communications capabilities. Once the technology matures and the standards issues are resolved, UWB could be used by public safety as a replacement for some of the cables and wires. Given that some chip manufacturers are developing plans to implement UWB on a chip, the impact that SDR may have in advancing this technology is unclear.

Non-terrestrial

Non-terrestrial communications principally consist of satellite telephone communications that provide coast-to-coast coverage for continental U.S. (CONUS) communications, provided line-of-sight (LOS) to the sky exists. Commercial satellite phones, such as Iridium and Globalstar, operate in the 1.6 GHz band and are capable of voice and data communications on a handset slightly larger than a cellular telephone. In some cases, the handset is even capable of switching from satellite communications to terrestrial cellular communications. The switching power of satellite phones could be enhanced through the implementation of full SDR. Public safety personnel would be able to maintain a wide area connection while responding to incidents where jurisdictional area network (JAN) coverage is not available. Commercial satellite phones do not have the indoor coverage and reliability required for first responders, and the airtime costs could be an issue, but the broad satellite coverage could be very valuable to enhance existing coverage.

Military

The other community of interest with whom the first responder community may require interoperability is the military. The JTRS response notes that “the JTRS Capabilities Deployment Document (CDD) includes development of an open standard Project 25 waveform application for Land Mobile Radio (LMR) communications. This waveform will evolve with

the Project 25 standard and provide interoperability between SCA compliant SDRs and the various proprietary Project 25 digital LMR communications systems that exist today." Although such development is vital to facilitating communications between first responders and the military, from a public safety perspective, the most cost-effective approach to implementing such interoperability is for the military to have public safety waveforms included in military radios that would be used for working with first responders.

3.3.3.3 Use of Services Other than LMR for Public Safety

Given the ability to utilize any of the services described above to interoperate with non-public safety users, another question to consider is use of such services for communications among public safety personnel. Numerous examples exist of use of (in particular) commercial wireless services by public safety users. In the United States, this is particularly true for broadband data. However, very few agencies rely on commercial wireless services for mission-critical applications, as public safety agencies require higher reliability than typically provided by commercial services for their consumer clientele. The flexibility that SDR technology provides could allow public safety applications that take greater advantage of commercial wireless services for voice and data (e.g., a first responder could easily reconfigure an SDR device to use a commercial operator when the public safety network is unavailable due to a network failure, lack of coverage, or some other reason). However, meeting the reliability requirements of public safety requires willingness on the part of the commercial providers to provide sufficient reliability (of network availability as well as terminal equipment) at a price point that public safety is willing to pay. Whether commercial wireless service providers can define a business case that would support such an arrangement, and whether the public safety community would be willing to adopt it, are open questions.

3.3.4. Conclusions

- The flexibility of SDR technology provides opportunities to take advantage of a rapidly growing set of possible communications protocols, network types, and so on. These capabilities may be important for first responders to communicate to non-first responders, and also could be used to handle first responder communications as well.
- Some challenging technical issues are significant cost drivers in development of single devices that include capabilities to access public safety LMR networks and other communications networks, such as cellular systems, Wi-Fi systems, and so on. These issues include frequency span (number of octaves as described in Section 4.4) and linearity.
- Commercial wireless organizations have an opportunity to position public safety as an application market by tailoring their product offerings to meet the incremental requirements posed by PS organizations. Government organizations have an opportunity to fund programs with specific public safety content and to work within organizations, such as the SDR Forum, to develop standards around those programs and promulgate information about them.

3.3.5. Recommendations

- Development of devices that include both public safety LMR waveforms and other services has consistently been identified as being of interest to the public safety community. Research and development work should be undertaken to address the technical issues of software implementations of non-linear public safety waveforms and other waveforms (such as commercial cellular) to determine the feasibility and cost trade-offs associated with the design of such devices.
- The Public Safety SIG should continue as a venue within which agreement between interested parties can accomplish the systems engineering and operational considerations needed to develop an approach to interaction between public safety radio systems and other domains to their mutual benefit. This is a win-win activity. Engaging the development and user communities within the Public Safety SIG and the SDR Forum provides the best potential for optimizing the functionality versus cost trade-off.

3.4. Ability to Meet Other Public Safety Requirements

Although interoperability is a key concern for public safety agencies, their communication systems must meet many other requirements. The SAFECOM Program has outlined 173 requirements for interoperable public safety communications. These requirements span a wide variety of areas including coverage area, reliability and interactions with other systems. Respondents were asked to comment on how SDR technology could address these requirements.

3.4.1. Areas of Consensus in the RFI Responses

- Only two detailed responses and one general response were received that addressed the question of SAFECOM requirements. Both responses indicated that the vast majority of the requirements could be met with existing or evolutionary technology development.

3.4.2. Areas of Divergence in the RFI Responses

- The responses disagreed as to the level of technology advance that would be required to meet some of the requirements. Notable responses are discussed in Section 3.4.3. The complete set of responses to the requirements is included in the Annex to this report.

3.4.3. Analysis and Discussion

Only three responses addressed the question of the SAFECOM requirements. The JTRS Program and M/A-COM responses addressed each requirement individually, and the Texas

DOT provided their high-level goals of desiring an inexpensive, multi-frequency, multi-mode SDR to better support their communications.

The RFI asked that reply comments indicate whether SDR technology that met the SAFECOM requirements was currently available, would be available in the near future, required a revolutionary technological advancement, or would not be available in the foreseeable future. JTRS and M/A-COM responded that of the 173 requirements, only six required a revolutionary technological advancement and four required technology not available in the foreseeable future. These requirements can be grouped into two categories: those that are dependent on SDR technological advancements and those that are dependent on general technological advancements.

Two requirements were identified as requiring revolutionary SDR technological advancements in addition to general technological advancements. The first of these, *the voice system must support real-time voice commands*, requires both general and SDR technology evolution. JTRS responded that the general capability to support voice commands is an evolving technology that can be readily integrated into an SDR-based system. M/A-COM agreed, but noted that extreme care is advisable to ensure the robustness and reliability of the algorithm.

The second requirement needing SDR technology advancement, *the system must be capable of interfacing with and/or controlling traffic control systems and the Intelligent Transportation System*, requires a maturation of both SDR and traffic control systems. JTRS replied that the controller is conceptually possible, but a new waveform would need to be developed for this application. M/A-COM agreed that additional network support would be necessary to meet this requirement.

JTRS and M/A-COM noted seven requirements that need revolutionary technological advancements, independent of SDR technology development, to be achieved:

- *The system must be capable of capturing data entered into the system in any manner, into any appropriate reporting forms* — JTRS replied that this is a requirement for a software application.
- *The public safety user/device must be able to communicate regardless of location* — M/A-COM replied that it was unlikely that SDR technology could meet this requirement because "ubiquitous coverage over practical, extended areas is impossible due to the laws of physics."
- *The communication system must be able to geo-locate the source of an attack* — JTRS noted that this would be protocol/environment dependent and did not appear to be a unique SDR requirement.
- *The communication system must be able to geo-locate the source of jamming* — M/A-COM indicated that this is a network support requirement.
- *The communications system must be capable of handling all top-priority traffic on a network simultaneously*—M/A-COM noted that "traffic handling capability is limited by the number of talk paths available for a given number of licensed channels." JTRS also indicated that there is significant communications protocol dependence.
- *The communication system must be able to continue to operate within the parameters set forth in 5.3.1 in harsh/hostile RF environments where the received signal level is*

less than -150dBm—M/A-COM indicated that operation in a harsh environment would require "revolutionary low bandwidth techniques…to reduce noise to this level."

- *The system must meet a minimum dependability of 99.999% within the context of the public safety communications system*—M/A-COM replied that "practical public safety designs cannot achieve area coverage of 99.999% without extreme cost."

Many of the SAFECOM requirements can or will be met by technology that is not inherently SDR technology but is enabled by SDR technology in order to meet the demands of public safety. For example, one requirement states that "the system must be capable of submitting automated database queries." The software to permit this function is not inherently SDR technology. However, because an SDR radio can support software applications, it enables this function to be performed on a radio instead of a laptop. Another requirement states that "the tone of the speaker's voice must be recognizable." The advancements in audio clarity through SDR technology could help meet this requirement.

No reply comments addressed the integration issues associated with SDR technology. These issues are another area that the Public Safety SIG can examine. As seen through the requirements, numerous technologies will need to work together to meet all of these requirements. SDR technology will only be a part of the greater system. Other technologies to be examined may include Intelligent Transportation System technologies, broadband communications, and geo-locating technologies.

3.4.4. Conclusions

- While the sample set of responses on this particular topic was small, we conclude that the vast majority of public safety communications requirements as defined by SAFECOM are achievable with evolutionary technology development.

3.4.5. Recommendations

- The Public Safety SIG should follow up this report with a review of updates to the *Public Safety Statement of Requirements* document to confirm and/or update this analysis with respect to the revised and detailed requirements.
- The Public Safety SIG should approach Project MESA to determine if there is mutual benefit in conducting a similar exercise based on defined MESA requirements. We anticipate that this dialog would be maintained informally through the public safety representatives that support both Project MESA and the Public Safety SIG.
- The Public Safety SIG should engage the TIA TR8 APIC Broadband Task Group and P34 user needs process.

4. CONSIDERATIONS FOR IMPLEMENTATION

The preceding section included analyses of key issues associated with the value of SDR technology to public safety applications. The conclusions in the discussion in Section 3 highlight the significant potential of SDR technology, but a number of issues and challenges exist in actually deploying the technology. These considerations for implementation are the focus of this section. Based on the questions and responses to the RFI, we have divided this discussion into five major issues:

- The overall strategy in technology deployment, specifically whether SDR should be deployed in terminal equipment or in system infrastructure;
- The role of standards in introducing SDR technology;
- The role of cognitive applications for public safety;
- Enabling technologies which must be advanced to fully realize the potential of SDR technology; and
- Security considerations.

Each of these topics is addressed in detail in this section.

4.1. Deployment—Infrastructure versus Terminal

Section 3.2 noted several different approaches to deploying SDR technology. One of the most distinctive differences in approach is whether to deploy the technology at the infrastructure or at the terminal. The Request for Information Question #2 included several questions relating to this topic, as follows:

- To meet public safety requirements, does SDR technology need to be implemented in both the infrastructure and the terminal devices?
- Are there advantages or disadvantages (technically, operationally, and/or financially) to focusing the technology in one of these areas?
- Which SDR capabilities are best suited for the infrastructure, and which are best suited for the terminal?

The responses to these questions are discussed next.

4.1.1. Areas of Consensus in the RFI Responses

- While the respondents diverged on the overall issue of infrastructure versus terminal (see Section 4.1.2), they agreed that if SDR technology was implemented in infrastructure, the implementation should begin with software definable gateway devices to connect different communications systems together. This form of implementation would provide the benefits of SDR technology to the most users quickly because there are fewer technology hurdles to overcome in developing such devices.

- The respondents agreed that an infrastructure implementation would initially bring the greatest benefit to users who, for budget reasons, must continue to use older, legacy terminal devices. Utilizing SDR technology in infrastructure can ease issues associated with migrating systems from older to newer technology.
- The respondents also agreed that implementing SDR technology in terminal devices would bring more direct benefit to the end user and would make SDR technology "user-centric.". They agreed that greater technology hurdles must be overcome when implementing SDR technology into terminal devices. Such hurdles include size, weight, power, and complexity of the unit.
- One of the respondents pointed out that SDR technology should leverage the power of standards such as the IP-based networking standards to realize the full potential of SDR interoperable technology, regardless of whether SDR is implemented in infrastructure or terminal devices.

4.1.2. Areas of Divergence in the RFI Responses

- The respondents diverged on whether infrastructure devices or terminal devices are best suited to be implemented initially with SDR technology. The respondents split nearly evenly on the question of which type of device provided the most benefit if initially implemented.

4.1.3. Analysis and Discussion

For the purposes of this report, infrastructure comprises the dispatch, system management, network transport, RF site, and basestation equipment, including deployable basestations. Infrastructure devices are used by the system. A terminal device is a device that is used at the subscriber side of the link (e.g., used by a person). Terminal devices can be further divided into a vehicular (mobile) category and a handheld (portable) category. Public safety typically uses the term "subscriber equipment" to refer to this definition of terminal. The mobile category is not as stringently constrained as the portable category by issues of size, weight, and power.

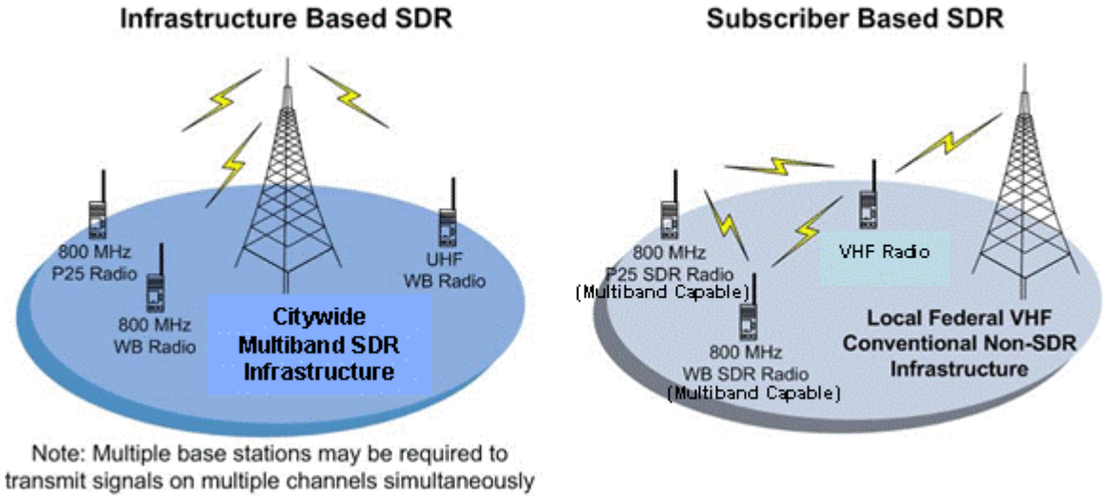

Figure 4-1
Infrastructure and Subscriber Examples

Implementing infrastructure-based SDR can be accomplished in two ways. The more beneficial but more complicated method would be to implement SDR technology into a single basestation that can accept a radio transmission and rebroadcast it over multiple frequencies simultaneously. As an example, Figure 4-1 shows the tower equipped with a single basestation originally configured for 800 MHz wideband transmissions, an 800 MHz narrowband radio, an 800 MHz wideband radio, and a UHF radio. Each of the radios receives identical, real-time transmissions from the SDR-equipped basestation.

The second form of infrastructure-based SDR requires a dedicated basestation for each additional channel for real-time voice communications. Since current technology cannot cost effectively multiplex multiple carriers in real time, each of the additional basestations would be used to rebroadcast the signal. Using the example described above, three basestations would be required to generate real-time signals for each of the radios shown in Figure 4-1.

Subscriber-based SDR, by which handheld radios can dynamically adapt to each surrounding radio's configuration, communicates seamlessly as a peer-to-peer network. This configuration, shown in the Subscriber-based SDR graphic in Figure 4-1, is a collection of interoperable SDR radios, originally configured to operate in disparate bands, communicating in real time either via the infrastructure or in a talk-around mode.

SDR technology in the infrastructure is important when new technology is introduced into the radio system. Most public safety entities cannot replace all equipment at one time and need to upgrade systems slowly as radios are replaced every year. When a public safety entity buys a new system, it typically has to provide connectivity to the old system until all users have received new radios and the new system has been verified. Having the capability in the infrastructure to support the "old mode" until the upgrade is complete and then to switch to the "new mode" at the touch of a button is an extremely useful capability that SDR technology can provide. This requires infrastructure and network support to realize the full potential of SDR technology. The end vision should be a system in which each user has an SDR terminal device that is easy to operate, especially in routine situations. These terminal devices should be supplemented by SDR devices in the infrastructure, which can take the management of complex

system communication tasks from the hands of the user and transfer it into the hands of the system operator.

Terminal operation must be kept simple for several reasons, including managing cost and minimizing operational complexity for the user. One approach utilizes a software programmable device that can easily be configured to set up communication pathways between two or more systems. This provides a large benefit to many system users at a minimal deployment cost. Doing so requires overcoming several technological, operational, management, and cost barriers. To separate these obstacles into more manageable pieces, the category of terminal devices should be divided into subcategories. A vehicular, or mobile, category of terminal device is one that is generally found in a vehicle. It is supplied with adequate power from the vehicle's electrical system and is not hyper-constrained by limits on its physical size and weight. A handheld, or portable, category of terminal device is designed to be carried by a person on foot. It has a severely limited supply of power available to it, generally from a battery integrated into its design. The handheld device and its battery are severely constrained by limitations on size and weight. Currently, the size and weight limitations must be overcome by application of new technologies, which require time to develop reliably and could add cost to the overall handheld product. Due to the large quantities of terminals involved in a typical public safety system, costs incurred in the terminal are multiplicative. This is one of the primary reasons that SDR terminal devices should be scalable, so that a public safety agency does not have to purchase many expensive devices that have unnecessary features that quickly increase the cost of the system.

Implementation of software radio in vehicular and handheld terminal devices would provide more benefit to users, in most instances, if the cost, management, and technology hurdles are successfully overcome. The technological hurdles for vehicular terminals are more easily overcome than those for handhelds due to the less stringent size, weight, and power constraints.

One respondent pointed out that SDR terminal units could be scalable, which would enable organizations with tight budgets to purchase devices with only the capabilities needed for each user, thus allowing the purchase of SDR terminals to be more cost efficient than the purchase of a few high-capability infrastructure devices. The general observation is that SDR allows greater flexibility in pricing models, which could benefit end users.

Another respondent pointed out that SDR terminal devices would allow individual users to roam among different systems while maintaining communication using their one terminal device.

4.1.4. Conclusions

- Implementing software radio technology as a flexible infrastructure and network device between systems provides an initial interoperability benefit for the least expense and within the shortest time period.
- Implementation of SDR technology is more readily accomplished today in the infrastructure.
- Implementation of software radio technology in terminal devices would provide more benefit to users in most instances once hurdles such as those concerning cost,

management, operations, and technology are overcome. Technology hurdles would be easier to overcome in mobile terminal devices than in portable terminal devices.

4.1.5. Recommendations

- A cost model should be developed for the terminals and infrastructure to better understand the cost implications associated with this question.

4.2. Standards

The responses to the RFI show that standards are a major consideration for SDR technology. Several of the RFI questions alluded to the effect and use of standards in SDR. This section covers responses relevant to the use of standards from questions 5, 7, 8, and 9 of the RFI, all of which addressed the question of SDR standards, such as the SCA and the Object Management Group (OMG) Platform Independent Model/Platform Specific Model (PIM/PSM). The RFI included several different questions on standards in an attempt to isolate the concept of standards for SDRs from specific activities undertaken by the military and the Object Management Group to define SDR standards. However, almost all of the respondents framed their responses similarly regardless of whether the question related to the SCA, the OMG Platform Independent Model/Platform Specific Model (PIM/PSM) or key components of the SCA, such as the Common Object Request Broker Architecture (CORBA) and eXtensible Markup Language (XML).

4.2.1. Areas of Consensus in the RFI Responses

- In principle, standardized system and/or component interfaces would be beneficial to public safety communication needs, although the responses showed significant divergence in what should be standardized and the details of such standards.

4.2.2. Areas of Divergence in the RFI Responses

- Some responses stated that JTRS SCA was not cost effective because it was designed to accommodate military requirements not needed by public safety. JTRS responded that there were potential advantages to adoption of the SCA since it is already in place and developed and, therefore, could be more readily leveraged for public safety applications. JTRS also noted that some specific features designed for military requirements could be removed from the SCA definition to align it with public safety applications.
- Some responses stated that public safety should consider products such as those being generated by the OMG Software Based Communications Domain Task Force. The JTRS Joint Program Office (JPO) pointed out that much of the JTRS architecture is designed using OMG procedures. In addition, some of these architectural issues are being addressed within the SDR Forum. Not all reply comments addressed the potential role of the OMG.

- There was divergence on whether the FCC position (that the hardware manufacturer is responsible for the total operation of the radio) is the best approach for public safety applications.

4.2.3. Analysis and Discussion

Standards are a consideration in several levels of software radio technology. They can apply from the component level of the radio, to the signals that the radio emits, to standards that define aspects of the radios themselves (such as the operating environment).

4.2.3.1 Concept of an Intra-Device Interface Standard

The first issue in standards concerns the level, degree, and application (e.g., protocols, APIs) at which standards need to be defined to maximize the benefit of SDR technology. The traditional public safety approach, reflected in such initiatives as Project 25, have focused standards definition at the interface between subscriber equipment and other subscriber equipment, subscriber equipment and infrastructure (e.g., the common air interface), or between elements of infrastructure (e.g. the ISSI). The JTRS program has taken a different approach, defining a standard architecture within radios (for example, within subscriber equipment) to facilitate the porting of software waveforms from one radio platform to another. Among the numerous differences between these approaches, the most fundamental is "where" the standard is defined and, specifically, whether there is a standard defined within a radio device. We define such a standard as an "Intra-Device Interface Standard," or IDIS, to emphasize that it is standard between components within a radio. The SCA is an example of an IDIS.

The first, most fundamental issue in consideration of standards for SDRs in public safety is whether an IDIS is beneficial. There are significant advantages and disadvantages with an IDIS in public safety radios.

The advantages of such a standard include ease of porting waveforms across different hardware platforms, additional competition, and the potential for innovation in development of waveform software as well as in development of hardware platforms. For example, standards facilitate the entry of companies with specialized capabilities into the market. Standardization around core architecture would allow manufacturers to specialize in creating different functionality for the device while knowing that, as long as it was built to the architecture specifications, their software would integrate into the device.

The advantages noted above come with a cost, however. System performance could suffer[19] because developers may not be able to take advantage of performance optimization across the entire device. Integration of potential multi-party components (waveform from one source, platform from a different source) could be more costly. Additional testing of integrated waveform/operating environment combinations would be required to meet the reliability and robustness requirements of public safety.[20] In addition, both the challenges of the standards

[19] Federal Communications Commission, First Report and Order, ET Docket No. 00-47 (FCC 01-264), September 14, 2001.

[20] The respondents did not address the question of an IDIS independent of the SCA. However, some of the advantages cited for the SCA, such as waveform portability and software component sharing, can be attributed to the SCA as an IDIS.

development process and the inherent limitations of a uniform definition can limit and slow down the flow of innovative capabilities into fielded equipment.

Introduction of an IDIS moves toward an "open architecture" SDR but raises a significant issue of accountability for the behavior of a radio that includes components from multiple sources that adhere to the standard. The FCC's *Report & Order on SDR* maintained the traditional responsibility of the hardware manufacturer to ensure that the radio would behave within regulatory limits. In the responses to the RFI and subsequent discussion within the Public Safety SIG, there was divergence of opinion as to whether the FCC position ultimately benefits public safety.

A number of approaches can be adopted in terms of defining responsibility for the behavior of the radio. One school of thought supports an "open" SDR, in which each contributor bears responsibility for the performance on his/her contribution. In practice, however, responsibility will most likely reside with the integrator (who could well be the manufacturer) who puts together the various elements to present it to the FCC for certification as a radio. The integrator/manufacturer could, in turn, hold its component suppliers accountable to the integrator/manufacturer. A user might not be permitted to download and use waveforms unless his "integrator" has already given approval for that hardware/software combination. This approach is consistent with a fundamental principle in the microeconomics of risk, wherein the best outcomes result when responsibility (liability) is placed with the entity in the best position to manage the risk. The reason for this approach is relatively simple: If an entity can effectively manage risk but is not held accountable for the realization of that risk, then there is a moral hazard that results in inadequate resources dedicated to risk mitigation.

The traditional regulatory regime and current FCC position is based on the notion that the greater the responsibility the manufacturer bears, the greater the degree of control the manufacturer must exercise over the device to manage the manufacturer's risk. The FCC position is that, without placing the responsibility with the manufacturer, it becomes more difficult to assign accountability of adherence to operation of the radio.[21]

In discussing the alternative perspectives, the Public Safety SIG agreed that the introduction of an IDIS would significantly change almost all aspects of how public safety radios are type accepted, procured, and tested. An IDIS, such as the SCA or the OMG Software Based Communications PIM/PSM, represents a radical departure from the current development models for public safety radios. The critical question to be resolved is whether such a departure is in the best interest of the public safety community and will be accepted by the vendor community.

Note that the concept of an IDIS is not to replace or run counter to the current ongoing standardization work in P25. The concept would include a P25 waveform that could be developed to meet the IDIS and used on IDIS-compliant radios with minimal modification. An IDIS might also facilitate the development of waveforms that interface with legacy radio systems. However, until proprietary waveforms can be licensed, the ability of next-generation SDRs to interface with legacy systems will be significantly limited.

[21] Note that the accountability issue can also make it difficult to assign responsibility if a radio does not conform with external standards, such as P25.

The two major alternative approaches to defining an IDIS for public safety are: (1) leveraging the SCA as currently defined as part of the JTRS program; and (2) developing a standard specifically for public safety SDRs not based on the SCA, but leveraging emerging commercial or de facto commercial standards if possible. Each of these options is discussed below.

4.2.3.2 JTRS and SCA

The Joint Tactical Radio System is a military communications program to develop and deploy software defined radios as the next generation of military radios. A key element of the design is the Software Communications Architecture. As described on the JTRS website:[22]

> the SCA is an open architecture framework that tells designers how elements of hardware and software are to operate in harmony within the JTRS. It governs the structure and operation of the JTRS, enabling programmable radios to load waveforms, run applications and be networked into an integrated system. Design engineers use the SCA definition document just as an architect or planner uses a local building code to design and build homes.

The SCA introduces advanced software technology into SDR using software technology standardized by the Object Management Group. The specific basis of the SCA includes the following OMG Standards:

- Common Object Request Broker Architecture (CORBA);
- Interface Definition Language (IDL); and
- Unified Modeling Language (UML).

The SCA also uses XML. The SCA places restrictions on developers to facilitate waveform portability. Waveform software is not allowed to make direct calls to the operating system and hardware devices, ensuring waveform implementation is independent of the specific execution platform. In many respects, the SCA is less about adding functionality (which can be done in the waveforms themselves) and more about forcing rules on how objects (e.g., APIs, CORBA, etc.) communicate with one another.

However, the SCA incorporates a key component of the SDR technology on which the JTRS program is based, and which could provide the basis of an IDIS for public safety. Note the distinction between the JTRS, which is a development and procurement program for military radios, and the SCA, which is a communications system architecture designed to facilitate interoperability and portability of software waveforms from one radio to another. Requirements of the JTRS for multiple levels of security and support for multiple waveforms executing simultaneously are not inherent in the SCA. In other words, a radio can be SCA-compliant but not meet the requirements defined in the *JTRS Operational Requirements Document.*[23] This distinction is important in discussing the application of the SCA for public safety and is often overlooked in assessing the advantages and disadvantages of the SCA.

---

[22] http://jtrs.army.mil/sections/technicalinformation/fset_technical.html?technical_SCA.

[23] Joint Tactical Radio Systems (JTRS) Operational Requirements Document, Version 3.2, JROC Approved, JROCM 087-03, 9 April 2003.

The JTRS Joint Program Office identified potential advantages of adopting the existing SCA in support of the public safety communications concept of the systems of systems as follows:

- "the ability to utilize an evolving architecture standard and set of system 'interfaces' which has had significant development expertise";
- "inherent capability to share various communication components (e.g., 'waveforms', system management tools, testing tools, etc.) across the range of communication environments";
- "ability to achieve market share leverage to drive costs down"; and
- "ability to incorporate evolving system management" and "cognitive radio strategies" (such as Type I encryption).

These advantages may be offset by disadvantages, however, particularly in the processing and memory demands on radio system hardware. M/A-COM noted that "new radio hardware would have to be designed, with an increase in the processing power and memory from the current industry products. This, in turn, will undoubtedly have a negative impact on cost, size, weight and battery life of the radio." In particular, the M/A-COM response notes that "the increase in processing power and memory is attributed to the overhead to support the platform independent software. CORBA, XML and the Core Framework are the most demanding components. These components add source code to both the platform specific and independent software. Similar proprietary implementations can be more efficient by simplifying the interface between the hardware abstraction and the radio application." These issues are of greatest concern in the potential implementation of portable units, for which public safety personnel may need to run on batteries for routine 8-12 hour shifts and for longer periods in response to major natural disasters or terrorist events.

M/A-COM also noted that the processing and memory penalties introduced by the SCA relative to a benchmark of current proprietary industry approaches have not been quantified. Thus, the true extent of the potential processing disadvantage of the SCA is not well understood at this time. As the performance implications of the SCA are quantified and if the SCA places untenable processing demands on radios from a public safety standpoint, an alternative approach to the SCA is development of a "lighter" version of the SCA. The concept of a so-called SCA-light is to leverage the development work that has led to the SCA by using the SCA as a starting point, and then removing required functionality that is needed to support military communications but not public safety communications. One analogy is to consider SCA-light as a version of the SCA in much the same way that Windows CE provides a lightweight operating environment based on Windows. The primary advantage of this approach is to mitigate the processing and memory penalties of the SCA while preserving most of the features that facilitate interoperability and waveform portability.

4.2.3.3 Non-SCA Intra-Device Interface Standards

The other alternative is to look outside the SCA as an alternative IDIS. For example, it may be feasible to define an Application Program Interface (API) standard within a device such that software waveforms could be written using generic standardized service calls that can be implemented in a variety of ways in the radio system. The advantage of this approach is that it provides the advantages of an IDIS without requiring that the radio operating environment be

implemented using CORBA, XML, and other elements of the SCA Core Framework. Note that no such interface standard has been developed, so any work in this area begins from scratch. The quickest approach to achieving this type of interface standard would be to leverage commercial standards. For example, implementation of a waveform on a commercial handheld computer (i.e., a system running something like the Windows CE operating system) is an alternative approach.

4.2.3.4 Other Standards

In addition to the IDIS issue are other standards issues to address, such as the degree to which external hardware and software interfaces to the SDR should be standardized. The outstanding question in this area is how the process of downloading new or updated software into the device can be standardized. This allows for uniformity when reconfiguring SDR devices. Other considerations include standardized interfaces on the device to allow modular design such that hardware devices can be added or deleted to meet the performance requirements of the device.

One of these standards involves the interfaces necessary to support software downloads. Any operational capabilities that depend on software downloads will require some standard interface protocols by which downloads are initiated, the format of the download, the integrity of the download, and so on. The public safety community can leverage ongoing work being performed by the SDR Forum in this area, but it needs to be compatible with other developments in wireless data in the public safety domain.

4.2.4. Conclusions

- The SCA addresses standard interfaces *within* a device. To date, the public safety community has worked toward standards between devices but not within a device. Therefore, introduction of an intra-device interface standard such as the SCA would make significant changes to the current business models and processes for development, deployment, and regulation of public safety communications equipment.
- The cost trade-offs and implications of adopting an IDIS are not well understood. The cost trade-offs of the SCA have not been quantified.

4.2.5. Recommendations

- Cost models should be developed to better characterize the relative costs and benefits of introducing an IDIS in the public safety domain.
- Additional research and analysis should be conducted to refine the regulatory regimes needed to effectively implement standards, particularly as part of the cost/benefit trade-off analysis of an IDIS.
- Additional research should be conducted to determine the feasibility of a version or variant of the SCA that would meet device requirements (processing, memory, power, and so on) for public safety. The Public Safety SIG should support the ongoing work in the SDR Forum to investigate an SCA-light.

- Additional research should be conducted to determine the feasibility of an IDIS designed specifically for public safety applications but not based on the SCA.
- Appropriate standards organizations including TIA, ETSI, IEEE, and OMG, should be engaged as part of the process of assessing standards feasibility. If feasibility can be established, standards should be identified and developed.
- Additional research should be conducted to identify the appropriate role of standards for software download.

4.3. Role of Cognitive Applications

Although so-called cognitive radios (CRs) are not specifically software defined radios, the flexibility of SDRs significant facilitates implementation of cognitive applications. Thus, the RFI included a set of questions to invite discussion of the role of cognitive applications for public safety. For purposes of this report, it is convenient to separate cognitive applications into two main categories, because the drivers and solutions are distinctly different. First, RF-related cognitive radio techniques are regulated by the FCC or other authority are of broad interest to all spectrum users and policy officials, and are most likely to impact external sharing aspects of public safety spectrum, although they could also be used for in-band efficiency improvements. Second, non-RF applications are primarily internal to the radios and the networks and fall into the category of "user features" of the devices. As such the implementation of such cognitive capabilities is generally dependent on the needs and preferences of public safety users, industry, and funding sources rather than external policies and regulations.

4.3.1. Areas of Consensus in the RFI Responses

- The first responder can better focus on the incident/threat by eliminating routine to complex radio operations through the use of CR applications to:
  - Be aware of its RF environment (e.g., vicinity of public safety incident);
  - Detect available and authorized RF resources;
  - Decide how to best operate within the existing infrastructure/network;
  - Automatically reconfigure and connect; and
  - Learn how to perform these steps better the next time.
- CR offers a broad range of RF techniques to choose from to improve performance, interoperability, efficiency, and so on, as well as many non-RF features that could greatly benefit the PS officer (e.g. automated sensor, self-healing/correction, translation).
- CR is becoming a significant concept for *all* future communications systems and devices for two fundamental reasons:
  - Its enhanced spectrum efficiency and improved access by making dynamic channel assignments, taking specialized measures to avoid harmful interference to others, and avoiding unused channel seconds.

  - The need for "intelligent" self-configuring, auto-adapting systems and devices that can handle the growth trend of complex waveforms and user requirements.

- Public Safety must carefully balance spectrum efficiency benefits against the critical need for system reliability, robustness, security, "instant on," and other unique requirements of the first responder.
- Appropriate and widely recognized definitions will facilitate consideration of CR techniques for public safety and the wireless industry at large.

4.3.2. Areas of Divergence in the RFI Responses

- Whether spectrum sharing can be allowed or is too risky for PS applications (example cites "spectrum pooling" as an advanced capability).
- Whether cognitive capability can be included in the same box as SDR for all potential applications and techniques or whether a separate box with a well-defined standard interface is required in some uses for at least the near future in order to avoid additional size, weight, cost and power concerns.
- Responses indicate differing "definitions/understandings" of cognitive radio.
- Whether PS radios must be absolutely deterministic in nature. If so, many optimization scenarios are precluded (see Section 4.3.3, next).

4.3.3. Analysis and Discussion

A significant portion of the seven responses to this question was of a general nature. For example, the response from the Ad Hoc WG provided an excellent account of the relationship between SDR and CR, a theoretical model describing the evolution from traditional hardware devices to the ultimate SDR, and some historical and current views on definitions and terminology. Comments by Datasoft refined and complemented the material on the SDR-CR model and made further suggestions for ongoing research and study. Because the material was not directly applicable to public safety operations and systems, the Public Safety SIG decided to refer this material formally to several other activities of the Forum (see below) for inclusion in their studies.

Most of the respondents included their description or "simple definition" of cognitive radio, to establish the appropriate context for the associated comments. This is due in large part to the lack of a widely applicable definition and it emphasizes the need for greater consensus on the preferred terminology both for the public safety community and the wireless industry in general. For purposes of this report, it is sufficient to view SDR as the device that is capable of modifying its RF parameters (frequency, modulation and/or maximum power, as well as any prescribed transmitting conditions) by using software after the device is manufactured. An SDR may also use software to modify games, ring tones, web browsers, and other non-RF applications, which are not regulated but are left to the choice of industry and users. As a logical extension to SDR, cognitive radio technology is a family of techniques, features, or protocols that can carry out various functions based on being aware of its environment, processing the information and deciding the appropriate or best action, and adapting its RF parameters

accordingly. It is expected that the technology will become increasingly intelligent, learning from past experiences and even providing "optimized" solutions and courses of action. As with SDR, many non-RF functions could be implemented with cognitive techniques; such features are not regulated but are left to the discretion and preference of manufacturers, users, and the sponsoring infrastructure.

In the RF domain, respondents recognized that CR can automatically adapt its RF use to a given location or specific incident, to a range of operational scenarios from presets for preplanned mutual assistance to complex on-the-fly disaster situations, and to assisting a first responder directly by performing complex RF configuration and connectivity tasks, allowing the officer to give priority to on-scene duties. Specific examples of "simple, low risk" techniques that should be considered include adaptive control of transmitting power and bandwidth. Notwithstanding potential and theoretical benefits, respondents were strong in their call for caution about RF-related measures that might increase the risk of harm to or any reduction of the current reliability and robustness of the existing PS system, such as spectrum sharing. In the non-RF domain, many examples were suggested: translation, self-healing, various types of environmental and personnel sensing, advanced security/safeguard features, power/battery management, and diverse networking functions. Some features in both domains may be implemented with relatively no additional weight, power, etc., as simple variations of typical circuitry, whereas other, more complex applications could be bulky or require significant power, negating any potential benefit.

4.3.3.1 Related SDR Forum Activities

In parallel with Public Safety SIG activities and in the same time frame as the RFI release and receipt of responses were several important developments and proceedings that related directly to the question on cognitive technology. Within the SDR Forum itself, the topic of cognitive radio has become a growing issue of interest since at least late 2003, leading eventually to a clear recognition of a natural progression from SDR devices to cognitive operations and techniques as linked wireless technologies. In November 2004, at about the time of release of the RFI on public safety, the SDR Forum undertook to include cognitive radio technologies within its mission and formally adopted two new groups to carry out studies: a Cognitive Radio WG under the Technical Committee and a Cognitive Applications SIG under the Markets Committee. The Public Safety SIG is working closely with these activities regarding Question #10 of the RFI.

4.3.3.2 Related FCC Activities

A second major activity involved the FCC, which initiated a proceeding in December 2003, "Facilitating Opportunities for Flexible, Efficient and Reliable Spectrum Use Employing Cognitive Radio Technologies" (ET Doc. 03-108). The resulting Report and Order (R&O), adopted March 2005, together with several comments from PS entities, provide a wealth of information, views and tentative conclusions that are directly relevant to this question. For the FCC and its management, there is strong policy interest and support for the early development and deployment of advanced technologies:

1. Cognitive radio is of huge importance to increased spectrum access, improved efficiency, and dynamic real-time spectrum usage;

2. Cognitive radio is applicable for all regulatory models—licensed, unlicensed and any new regime—while reducing the risk of harmful interference to other users;
3. Cognitive radio is closely linked to SDR and already in use in many simple implementations, such as cordless phones, cellular networks, and WLANs;
4. Further deployment of increased computer processing capabilities in SDRs is expected to accelerate the development and use of CR techniques; and
5. Goals are to ensure rules and policies do not inadvertently hinder development, to enable realization of the full range of potential benefits, and to pursue new or clarified rules in an evolutionary fashion.

CR applications that were identified for current and near-term use and that appear to have potential benefit for public safety operations include frequency agility, adaptive modulation, transmit power control (TPC), and location awareness. For the long-term future, the R&O noted that some parties (e.g., DARPA's XG Project) envision revolutionary new "smart radios" operating on an opportunistic basis, finding idle spectrum, using frequencies as needed, then vacating the spectrum for others to use, all without human intervention, harmful interference, allocation tables, or regulatory bodies. However, the FCC referred to such proponents as "futurists" and declared that the model would involve many technical, cost, and business issues that would require marketplace resolution before implementation and, hence, the FCC is not addressing such changes now. Finally, it should be emphasized that the FCC identified three specific CR-based approaches for possibly implementing interruptible/secondary shared use of licensed spectrum, which has been consistently associated with secondary markets to take advantage of the perceived "bursty" low-average use of the PS bands.

Specific comments on cognitive radio were filed by several PS entities, as follows:

NPSTC

- Additional safeguard rules are required for specific high-risk threats (e.g., ability to affect many transmitters via Internet), whether by CR/SDR device or not.
- Secondary market/sharing with the PS concept is flawed because it assumes excess spectrum and that lessees will accept long interruptions for wildfires or such other situations.
- The FCC concept of the PS interoperability requirement is inaccurate.
- Dynamically coordinated spectrum sharing is not applicable to PS operations.
- The pre-certification testing process is essential for proof of concept and compliance.

APCO

- The interruptible spectrum leasing concept for PS is flawed.

New York State/Statewide Wireless Network

- CR is a subset of SDR—not vice versa—but they are not regulated the same.
- The use of some techniques is not directly applicable to PS operations (e.g., non-uniform channel plans in some bands and mix of trunked/conventional systems).

- Adaptive modulation and TPC are especially beneficial for public safety.
- Spectrum leasing (via CR-based techniques) raises many concerns.

St. Clair County, Illinois

- Cognitive radio has the potential to enable efficient, reliable and interruptible sharing of the PS spectrum with commercial users, assuming adequate reversion when needed.
- The lease of unused PS spectrum could help fund new technologies/systems.

4.3.3.3 Cognitive Applications to Spectrum Efficiency and Performance Optimization

From a public safety perspective, the applications to spectrum efficiency need to be investigated but carefully implemented. While cognitive techniques may provide a more viable approach to spectrum efficiency than continued narrowbanding (to 6.25 kHz channels), implementation could be risky or even detrimental to documented communications and interoperability requirements. In particular, the concept of interruptible spectrum leasing, which could be implemented by CR functionality, bears special attention—several public safety organizations expressed strong concern and objection to the FCC.

Analysis of public safety spectrum usage must account for public safety's stated need for near-instant (less than 250 milliseconds[24]) channel access for any push-to-talk (PTT) action. Due to the life-critical nature of public safety communications, typical PS requirements dictate that, for a trunked radio system, the probability of delay-producing queues (i.e., grade of service, or GOS) must be maintained to an extremely low value, often less than 1% for any PTT during the *busiest hour* of operation. The implication of this requirement is that for only 1% of the time can all channels of a public safety trunked system be simultaneously occupied by calls during the busy hour. This imposes an important upper bound on usage of the public safety frequencies that must be factored into any analysis of public safety spectral utilization. Certainly, conclusions regarding the utilization of public safety spectrum must recognize this important requirement.

Another key issue in the ability of cognitive techniques to enhance spectrum efficiency is the ability to detect interference. While the FCC is currently deliberating regulatory approaches, it is worth citing the public safety experience in identifying and documenting interference in the 800 MHz band over the past several years. The public safety community found it very difficult to conclusively identify and document the source of specific interference problems even when the interfering transmitters were fixed and performing in a known (licensed) manner. The challenge of avoiding interference in a more dynamic environment is formidable, with severe consequences if public safety mission-critical communications are compromised. These issues suggest that sharing allocated public safety spectrum outside of public safety control faces significant technical hurdles.

Most such studies are based on the assumption that users' demand for spectrum is uncorrelated. In other words, when any given user utilizes spectrum for communications, other users are not more nor less likely to demand access to spectrum. Under this assumption,

[24] *Statement of Requirements for Public Safety Wireless Communications & Interoperability,"* The SAFECOM Program Department of Homeland Security, Version 1.0, March 10, 2004.

spectrum utilization is most efficient when users who typically communicate in one band are able to utilize other bands during periods of peak demand.

However, considerable anecdotal evidence exists that this assumption does not hold with respect to public safety. In particular, during major events, first responders need to coordinate incident response at the same time news media demands for spectrum increase, commercial subscribers desire to tell loved ones of their safety and whereabouts, and so on. If spectrum demand is highly correlated, as such anecdotal evidence suggests, then economic and technical bases for sharing spectrum may be inappropriate for public safety applications. Unfortunately, researchers have not conducted a comprehensive quantitative study of spectrum demand across public safety and commercial wireless domains during both routine circumstances and incidents. In addition, the preceding examples are oriented toward voice communications, and the interaction of demands for voice and data communications contributes additional complexity to quantifying spectrum demand. Without such data, the impact of sharing spectrum that affects public safety cannot be adequately anticipated.

In mid-2004, the SDR Forum Public Safety SIG decided to seek a better understanding of spectrum usage in PS and certain other bands through the collection of quantified monitoring data during routine, pre-planned events and emergency incident situations. The Public Safety SIG assisted in the planning for a major collection effort across all services in the 30-3000 MHz band in New York City during the Republican Convention, 30 August–01 September 2004, performed by the Shared Spectrum Company and Stevens Institute of Technology. The results, and results from similar efforts around the world, are expected to provide a body of data that will support activities in spectrum planning, sharing, and usage modeling, as well as contribute to setting excellent criteria for evaluating and developing new technologies—SDR and CR—for the public safety sector.

As a final note, although the original motivation for cognitive radios was spectrum efficiency, a number of additional potential applications of the technology in the broader context of performance optimization exist. Performance enhancement could include capabilities such as adjustments to voice quality, capacity adjustment, real-time selection of routing and service based on variable parameters (e.g. lowest cost, highest reliability, fastest call setup). As SDR technology evolves in the marketplace and cognitive technologies mature, more effort will be appropriate to determine how public safety communications can benefit.

4.3.4. Conclusions

- Cognitive radio will become the wireless norm over the coming years for applications including public safety.
- Cognitive applications offer public safety significant potential benefits, even if improved spectrum efficiency and dynamic spectrum access are not the strong drivers, as they are with other user groups and radio services.
- If the cost is reasonable, cognitive radio technology will be incorporated in any and all new systems, where appropriate. (Note: Many would contend that simple CR is already deployed.)

- As SDRs become more capable and complex, the use of cognitive radio techniques to manage complexity will become more appealing and compelling.
- The definition issues need to be settled.
- There is a need to build a body of quantified data on spectrum utilization across all services (e.g., public safety radio services, commercial services, other private wireless services, federal government, etc.) during routine, pre-planned event, and emergency incident situations. Collection and analysis will require specialized data collection equipment development. These data would support spectrum planning, sharing, and usage modeling activities.

4.3.5. Recommendations

- The Public Safety SIG should monitor and assist in the SDR Forum's work on cognitive radio definitions, currently under way within the Cognitive Radio Working Group and Cognitive Applications SIG.
- Research should be undertaken to collect, document and analyze additional spectrum usage monitoring data.

4.4. Enabling Technologies

The full potential of SDR for public safety will not be realized without the continuing advancement of several key radio technologies. One of the goals of the Public Safety SIG is to identify the technologies that are the most important to achieving the benefits of SDR for public safety. This identification will enable a better understanding of the limitations imposed by critical technologies on the realization of SDR's benefits and facilitate identification of technologies that should receive enhanced development focus by the Public Safety SIG. To this end, the Public Safety SIG solicited responses from industry to the following question:

- What enabling technologies (e.g. antenna technology) are also required to realize SDR benefits?

Table 4-1 summarizes the input from the eight industry reply comments to the above question. In the table, the placement of the Xs directly below a particular industry that submitted a reply comment indicates the technologies that the reply comment identified as being enablers for SDR. The technologies are listed in order, with those having the most reply comments as SDR enablers listed first.

Table 4-1
Industry Responses for SDR Enabling Technologies

	Motorola	*M/A-COM*	*Thales*	*JTRS*	*HYPRES*	*Ad Hoc WG*	*Texas DOT*	*DataSoft*
Antennas	X	X		X			X	X
Front-ends	X	X	X	X				
A/Ds and D/As		X	X		X			
Digital processors and memory	X	X	X					
Wideband/ baseband	X							
Standards-based communications strategy and protocols				X				
Efficient batteries	X							
Human-machine interface			X					
Non-physics technologies, such as supplemental protocols				X				
Development time							X	
Costs							X	
Vision						X		
Technology to implement end-to-end video delivery across a mobile wireless network								X
Biometric and other authentication techniques								X

4.4.1. Areas of Consensus in the RFI Responses

- As Table 4-1 indicates, the following technologies were each mentioned by three or more reply comments as being key SDR enablers:
  - Front-ends;
  - Multi-band antennas;
  - A/Ds and D/As (sampling technologies); and
  - Digital processors and memory.

The other technologies listed in Table 4-1 were each mentioned in no more than one reply comment.

- Of the above four most-mentioned enabling technologies, it was the general consensus was that advances in digital processing have outpaced RF front-ends, multi-band antennas and A/Ds and D/As. Digital processing/memory has benefited the most from Moore's Law advances in speed and density, whereas the other three key enablers require substantial further improvements before SDR can reach its full potential.
- In regard to processors and memory, two of the reply comments discussed the criticality of speed, size, weight, cost and battery life trade-offs for a public safety radio design and how these trade-offs limit the choices of what SDR devices can be used practically in the radio. Cost, size, weight, power, and speed trade-offs dictate that many processing devices don't make sense for portable implementations, primarily due to excessive power consumption.
- Three reply comments discussed the criticality of A/D and D/A converters in the ability to achieve advanced SDRs, with the converters operating near the antenna. HYPRES mentioned that "SME implementation of Digital RF capability far exceeds the performance levels of traditional circuits and opens the way to consideration of new architectural enhancements." However, another reply comment indicated that cryogenic cooling required by such high dynamic range RF sampling devices would probably be impractical for implementation in a portable device.
- Many reply comments alluded to the advantage of having a single antenna capable of operating across the full frequency range of a multi-band SDR, and that traditional passive antennas limit the range over which an antenna functions effectively. The combination of multiple RF bands into one antenna must be accomplished in a small form factor, which traditionally has lowered the antenna's efficiency and, thus, reduced the battery life. One reply comment mentioned that developments in actively tuned antennas would alleviate this limitation. Related to tuned antennas, another reply comment stated that microelectromechanical (MEM) antennas controlled by software might facilitate the requisite gains in efficiency for such implementations.
- JTRS mentioned "non-physics" technologies, such as those related to improving quality-of-service (QoS) through the use of supplemental communications protocols, as being key SDR enablers. JTRS also asserted that the use of a "standards-based"

(such as the JTRS SCA or the OMG Software Based Communication PIM/PSM.) communications architecture strategy is an "enabling technology" in and of itself.

- The complete responses from all industry participants are found in the Annex to this report.

4.4.2. Areas of Divergence in the RFI Responses

- As shown in Section 4.4.1., the reply comments of the eight respondents identified a variety of different SDR enabling technologies. However, there was no divergence of opinion regarding any of the individual technologies.

4.4.3. Analysis and Discussion

Moore's Law advances in digital processors and memory have been the most influential factor for the proliferation of new SDR architectures. The processors can be implemented using individual or combinations of digital signal processors (DSPs), general purpose processors (GPPs), configurable computing machines (CCMs), Field Programmable Gate Arrays (FPGAs) and, to a lesser extent, application-specific integrated circuits (ASICs).[25] Portable size, weight, cost, and battery life trade-offs tend to favor DSPs for performing high-speed processing in a public safety radio, typically in combination with a GPP for slower radio control and user/external interface functions. The advances in these processor and memory technologies have enabled present-day public safety radios to support multiple operating *protocols* in the same radio. For example, today's public safety radios from the major manufacturers typically include P25, analog-FM and the proprietary protocol(s) of the manufacturer. This trend is expected to continue for even more functionality and additional operating protocols as radio processor and memory developments continue to track the Moore's Law curve.

In contrast to the rapid advancements that have been made in processors and memories, RF and analog components have not benefited from Moore's Law, and thus have progressed at a much slower pace. Such technologies include, but are not limited to, high speed and dynamic range A/D and D/A converters, multi-band antennas, and the radio's front-end RF components. For example, trade-offs of performance, size, weight, cost, and power consumption indicate that today's front-end technologies are deficient for implementing higher than a Tier 2[26] public safety radio. These deficiencies have caused the implementation of multiple bands in a single radio to be a greater technology challenge than implementing multiple protocols, especially if the bands are separated in frequency by one or more octaves. The insufficiency of these technologies is exacerbated for portable implementations that require low-power devices as well as by public safety's stringent RF performance requirements.

For a portable implementation, A/D and D/A converters are a significant limiting factor in progression toward the ultimate software radio, with a need for converters with the requisite

[25] Although ASICs have the lowest power consumption and highest speed, they tend to have fixed functions, and thus lack the programmability needed for SDR. The cost of new ASICs in a public safety radio can be high compared to, for example, the use of ASICs in a cellular radio because the non-recurring expense (NRE) of development is apportioned to fewer quantities of manufactured units.
[26] See definitions of tiers in Section 2.2.

combination of low power consumption (for a portable), high sample rate, and high dynamic range. Furthermore, at present, no major breakthroughs are anticipated for portables from A/D converter technology to mitigate this problem, at least not in the near future.

Also, advances are needed in bandwidth capability of low-cost front-end RF amplifiers as well as multi-band antennas with the requisite small form factor for portable implementations. The gain-bandwidth product of amplifiers and the antenna at the RF front-end will also need to improve greatly for efficient operation over multiple bands. For portable operation, the combination of multiple RF bands into one antenna must be accomplished in a small form factor, which traditionally has lowered the antenna's efficiency and thus reduced the battery life. There is hope that MEMs controlled by software will facilitate the requisite gains in efficiency for such implementations. Some companies are reportedly developing multi-band antennas that use MEMs, varactors, and software algorithms to tune a small portable antenna for efficient operation over multiple bands. Other work is being performed in using artificial magnetic conductor (AMC) surfaces to increase the bandwidth of flush-mounted wire or strip antennas.[27] The "best" implementation of a small form factor, high efficiency, portable, multi-band antenna is yet to be determined.

To mitigate these RF front-end technology deficiencies in the realization of multi-octave band operation, an alternate architecture to that of a Tier 2 or higher SDR design is to use separate RF front-end circuitry in the radio for each band. Also, if the bands are close in frequency (such as a dual-band 700/800 implementation), the aforementioned front-end technology problems are not as severe because the percentage bandwidth requirements of the front-end components are lessened. The physics of multi-octave processing presents a particular challenge for public safety radios, as the frequency bands range from low-band (below 50 MHz) to above 800 MHz,, and the public safety bands do not overlay another market from which public safety could benefit. One approach to introducing the technology into the market is for public safety to consider trade-offs of various band groupings to decide on what groupings result in cost/benefit breakpoints. For example, a radio that implements a grouping of the adjacent 700 and 800 MHz bands will likely be less costly than one that implements a grouping of VHF and 800 MHz that are separated by more than two octaves in frequency. However, the cost/benefit trade-off analysis must also consider any advantages of the latter grouping to the user that might outweigh the additional expense.

SDR is also a key enabler of advanced signal processing algorithms that can be used for various purposes in a radio, including compensation for hardware inaccuracies or inefficiencies. An example involves the use of SDR to compensate for nonlinearities introduced by the radio's transmitter hardware.

To achieve higher-speed data capability and/or more talkpaths per channel, multi-level modulations offer an advantage in spectral efficiency but often at the expense of requiring linear transmitters. The primary limiting component in achieving transmitter linearity is the power amplifier (PA). In most of today's public safety radios that use constant envelope modulations, the PA operates in a saturated, non-linear mode for achieving maximum power efficiency. To achieve the requisite linearity, the output power can be reduced to the linear range of the PA (at

[27] "Broadband Antennas over Electronically Reconfigurable Artificial Magnetic Conductor Surfaces," Antenna Applications Symposium, September 19–21, 2001, Victor C. Sanchez, Titan Systems Corporation; William E. McKinzie III et al., Arizona State University, http://www.etenna.com/literature/conference_papers/.

the expense of reduced coverage range and/or higher power consumption) and/or the nonlinearity introduced by the PA can be compensated using signal processing algorithms external to the PA. Two well-known techniques for accomplishing external compensation that can be implemented in the software of a SDR include Cartesian feedback loops and digital predistortion. Such PA linearization techniques are more efficient than power backoff alone; furthermore, they achieve the advantages of potentially lower cost and greater precision, repeatability, and flexibility.

4.4.4. Conclusions

- The industry responses and the discussion in the previous section support the conclusion that front-end RF, multi-band antennas and front-end sampling technologies are critical and also in need of accelerated development to realize the full potential of SDR.

4.4.5. Recommendations

- The SDR Forum should devote continued emphasis on studies and promotion of these technologies, making sure that the requirements for the public safety frequency bands are an integral part of the RF technologies thrust to help ensure that the developers of these technologies are cognizant of public safety's requirements.
- Research should be conducted to characterize the cost/benefit trade-offs of frequency band and service combinations with respect to public safety requirements. This research can then be translated into SDR development efforts that focus on those combinations that are most cost-effective for public safety applications.
- Public safety should consider any possible device synergies with other users of frequencies at or near the public safety bands. Devices that support multiple waveform types that are closer in frequency (e.g., within an octave) simplify the device front-end and may allow components to be developed over a broader user market.

4.5. Security

The RFI did not pose any questions specifically related to security, but in subsequent analyses of the responses, it became apparent that security is a major concern that must be addressed for the application of SDR technology in the public safety community to be successful. In particular, security may be an important component of what might be standardized to achieve maximum portability among hardware and software components and interoperability between communicating radios.

4.5.1. Areas of Consensus in the Discussion of RFI Responses

- Security is critical to public safety radio because failures, such as successful attacks on radio functionality or compromise of information, could gravely impact the lives of public safety users and the people they serve.
- SDR security mechanisms should be consistent with P25 and other security protocols being developed by the public safety radio community.
- Security mechanisms in public safety radios must be interoperable.
- Security technology could impact functionality if not properly implemented.

4.5.2. Areas of Divergence in the Discussion of RFI Responses

- Within the Public Safety SIG there is significant divergence over what cryptography and key management mechanisms might be appropriate for public safety applications.

4.5.3. Analysis and Discussion

The focus of this report is on security issues associated with SDR and the issues with integrating measures for ensuring the integrity and reliability of the radio software with other security issues associated with public safety communications (e.g., security of voice and data transmission, reliability of the radio, and so forth).

Security threats to public safety SDRs can occur in two situations: (a) run-time (when radio communication occurs) and (b) non-run-time (when the radios are not in use, such as when they are undergoing maintenance, are being kept ready for deployment, or are remaining inactive in a first responder's vehicle or office). The run-time case is the most critical because this is when radio functionality is needed immediately. The non-run-time case is also important, however, because during this time malicious software can be downloaded onto the SDR device, which can then affect the security of their operations at run-time.

Information and communications security generally involves five major areas: authentication, confidentiality, integrity, availability, and accountability. Varying definitions for these terms exist; they are briefly defined here in the context of SDR:

- *Authentication:* Ensuring that software loaded into the radio is from a trusted source.[28]
- *Confidentiality:* Hiding content from unauthorized users, such as those eavesdropping on radio links.
- *Integrity:* Protecting downloaded software from tampering.
- *Availability:* Ensuring that radio communication can occur on demand.

[28] User authentication may be needed in addition to software authentication to ensure that the user is authorized to obtain the software. In general, user authentication issues are the same between hardware and software-based radios, but recent research in cognitive applications is devising mechanisms to determine the identity of a radio user based on behavior rather than traditional forms of authentication, such as personal identification numbers.

- *Accountability:* Ensuring that software download and other transactions can be traced back to the parties that engaged in the transactions in such manner that the sequence of transactions can be recreated and that parties cannot later deny their participation.

Table 4-2 identifies key issues in each of these areas with respect to public safety communication. The remainder of this section addresses each of these security areas in more detail.

Table 4-2
Security Issues in Public Safety Radio

Security Objective	General SDR Issues	Public Safety-Specific SDR Issues
Authentication	• The source of radio software should be authenticated before that software is permitted to operate. • User identities may also require verification in many applications.	• Incident commanders need the ability to override authentication controls if they pose an immediate risk to life or property. • Authentication transactions must still occur even when significant portions of the network infrastructure have been destroyed or are otherwise unavailable. • Public safety radio users should be able to authenticate radio software and users from organizations with which they may have had no operational relationship prior to an incident.
Confidentiality	• Software vendors may need to protect trade secrets and intellectual property (e.g. digital right management).	• Confidential requirements vary within the public safety community. Law enforcement users typically have greater confidentiality requirements than other areas of public safety. Much of public safety communication is considered public and therefore does not require confidentiality protections. However, law enforcement routinely secures communications related to sensitive operations.

Security Objective	General SDR Issues	Public Safety-Specific SDR Issues
Integrity	• Strong integrity protections are needed to protect against viruses, worms and other forms of malicious code that could impact SDR functionality. • Because many software applications may be downloaded over-the-air, integrity checks of the software are essential (to verify that correct software has been loaded and installed).	• Public safety likely places a higher value on software (and system) integrity than most applications of commercial SDR due to the potential impacts of integrity failures for human life. • From a technical perspective, the general methods of integrity protection are likely to be very similar across all sectors.
Availability	• Because software radios are reconfigurable, they are inherently more subject to failure-inducing changes that could impact the availability of radio communication. • SDR technology represents both a threat and a solution to radio interference problems. Greater radio flexibility means that more users will have the ability to cause interference not commonly experienced today. Conversely, SDR technology can better support countermeasures to radio interference, by using techniques such as frequency hopping and multi-path routing.	• SDR availability threats and countermeasures are similar across public safety and other sectors. • Public safety has greater availability requirements than commercial wireless and other sectors due to the nature of the public safety mission. • Public safety radio operates in dedicated frequency bands so it is potentially less impacted by interference issues than radio applications that use shared spectrum. • In emergency situations, public safety radios should be able to use other, normally unallocated, frequency bands and other communication resources to ensure as high degree of availability as possible.
Accountability	• Regulators, manufacturers, and consumers all have an interest in ensuring that relevant parties are accountable for radio transactions, especially when radios are reconfigurable.	• Many public safety applications have specific legal requirements regarding the ability to trace, audit, and recreate communications transactions, including downloading software.

Note that there are additional security issues associated with public safety radios, such as authentication of the users and the ability to disable or remotely remove a radio from the network (e.g., if a radio is stolen). These security issues are not included in Table 4-2 because they apply to all radios, SDR or not. The critical consideration is to ensure that SDR does not adversely impact security solutions that are integrated into current (non-SDR) public safety radio networks.

Also note that security concerns are compounded in multi-service radios that expose SDRs to networks that may not be controlled by public safety. Unless uniform security protocols are in place, the security of the system (from a practical perspective) reverts to the least secure of the networks being accessed.

4.5.3.1 Authentication

A major new threat introduced with SDR is the potential distribution of malicious radio software, which could compromise communication or render radios inoperable, with especially harmful consequences in times of crisis. Whereas modifying the radio behavior of a traditional radio requires physical presence and operation on one device at a time, SDR technology enables an attacker to nearly simultaneously affect multiple radios on a network. Although hardware-based attacks can be prevented with physical security (e.g., keeping the hardware radios under lock and key), preventing software-based attacks requires some form of identity verification. The two leading proposed approaches to providing authentication services are digital signatures and trusted networks.

- *Digital signatures:* The entity providing assurance for the software (typically the developer) digitally signs the radio code. The radio verifies the signature during the download transaction and perhaps at run time as well. This approach requires a public key infrastructure (PKI). Public safety entities would need to trust a common certification authority to share their radio software. Open questions for the public safety community are who would develop the PKI and how it would function in practice.
- *Trusted networks:* Public safety users would trust radio software because it is downloaded from a trusted network to which they must authenticate. The trusted network approach is problematic in ad hoc environments (such as those established for a multi-agency incident response) if users must authenticate to a network for which they have no pre-existing credentials.

Members of the Public Safety SIG have disagreed over what cryptography and key management mechanisms might be appropriate for public safety applications. Some believe public safety communications requirements, including the need to operate the system when centralized security infrastructure has been destroyed, would necessitate the use of public key cryptography and, therefore, a PKI. Others suggest alternatives to public key cryptography should be explored. One radio manufacturer has suggested that PKI's complexity had the potential to cause operational problems that could be mistakenly blamed on the manufacturer even if the issue resulted from failures in a third-party's implementation of the PKI. The issue of legal liability was raised.

4.5.3.2 Confidentiality

Many radio manufacturers and third-party software developers will want to prevent unauthorized parties from obtaining both source and executable radio code to protect trade secrets and intellectual property. Some public safety agencies may also want to prevent local adversaries from obtaining radio software in order to prevent them from using that software to disrupt communications or obtain intelligence on their operations. The PS SIG, however, recognizes that many public safety organizations do not have such a confidentiality requirement. When confidentiality services are needed, they can be provided under both the PKI and trusted network paradigms discussed above. In the PKI model, additional public-private key pairs can be generated to encrypt radio software. In the trusted network model, a variety of methods can be used to encrypt either particular network links or end-to-end communication between the radio and the server hosting the radio software. However, many of these methods used on trusted networks also rely on PKI technology to distribute the keys necessary for the encryption.

4.5.3.3 Integrity

Integrity is critical for all SDR applications due to the fact that, if the radio code can be modified in an unauthorized fashion, just about any adverse consequence possible can soon follow. Integrity must be protected in both the run-time and non-run-time states. Digital signatures provide integrity services as well as authentication. Trusted networks, in contrast, can provide integrity during the download transaction but not after installation of the software. In that case, additional mechanisms, such as cryptographic hash capabilities, must be incorporated into each SDR device to provide the integrity function.

4.5.3.4 Availability

One of the major threats to the availability of communications is radio interference. Persistent intentional radio interference constitutes a denial-of-service attack on radio communication. Unfortunately, it is practically impossible to completely eliminate the risk of a denial-of-service attack due to the fact that an adversary intent on jamming signals can do so if it is in possession of a transmitter with sufficient power. Nevertheless, some countermeasures do exist, such as frequency-hopping (to counteract jamming) or multiple-path routing (to avert flooding at specific routers).

One area in which SDR technology likely will provide superior capabilities relative to that for hardware radios is multiple-path routing, which offers a solution to some difficult radio interference problems. Spread spectrum multiple-path routing may provide increased reliability. However, multiple-path routing may come at the cost of increased spectrum usage. This routing layer technique does not necessarily require additional spectrum, but it uses more links and channels of the already existing network. Emergency time invocation of the additional spectrum usage for enhanced reliability will require some policy and regulatory changes, justified by the need to support emergency operations (just as fire trucks have the right of way through a street crowded with traffic). Multiple-path routing techniques essentially deploy parallel, independent routes between the sender and recipient and can offer the high degrees of reliability required for PS radios.

In the future, another countermeasure to interference-based denial-of-service attacks may be to procure devices that are frequency agile and have adequate “cognitive” capability. These

radios would find new frequencies when public safety bands are jammed. However, the technical innovation and regulatory reform needed to support this capability will likely occur after adversaries gain the capability to cause interference using SDR.

Although the above discussion has focused on intentional interference deliberately intended to impact radio system performance, the cognitive capabilities and countermeasures described above will mitigate unintentional interference as well.

4.5.3.5 Accountability/Non-Repudiation

Determining who might be responsible for communications problems or regulatory violations is more challenging for SDR than for hardware radios because SDR devices are reconfigurable, whereas the general operating parameters of hardware radios are more or less fixed. Accountability with SDR depends on the ability to tie transactions to particular identities and on the ability to record those transactions. The first of these abilities is achieved through authentication, and the second through an event-logging or audit service.

As discussed above, authentication of software can be achieved through digital signatures or trusted networks. In general, authentication methods that rely on PKI offer superior accountability (or non-repudiation) properties because in no case should an entity's private key be shared, and thus all transactions performed with that key can be traced to a single source. In any shared secret mechanism (e.g., passwords or symmetric keys), however, at least two parties must share the secret, which means that any party to a transaction could potentially claim that some other party was responsible for that transaction.

Recording transaction information in an event or audit log also achieves a certain degree of accountability. Some issues related to audit systems include:

- What events should be logged;
- How much information about an event should be recorded to adequately capture it;
- Who has permission to read or clear the audit logs;
- How long audit records must be retained; and
- Whether the information is stored locally or transferred to another device.

Many public safety agencies have specific legal requirements regarding audit records. They may have to expand audit rules or guidance to address SDR transactions that are not covered in current systems.

4.5.3.6 Other Considerations

In addition to the "traditional" security issues outlined above are several security considerations for public safety SDR applications, including:

- Software quality assurance;
- The need for the ability to override security controls; and
- The implications SDR capabilities have outside of the public safety community on public safety communications.

Each of these considerations is addressed below.

Software Quality Assurance

The primary security control for SDR discussed above is authentication of the source of downloaded radio code, whether that occurs through a digital signature mechanism or by connecting to a trusted network. The basic problem with this approach is that knowledge of the source of radio code is not proof that the code is in fact secure. Rather, this knowledge is merely supporting evidence that the code is *likely* to be secure based on past experience with that software manufacturer or confidence in its brand in the marketplace. A substantial risk still exists that the code still has significant vulnerabilities, perhaps due to inadvertent mistakes in the software development process or even as a result of a rogue employee in the organization that developed the software.

Ideally, public safety agencies should have some additional assurance based on certification of the development process used to create the code or testing of the code itself. For instance, the reliability requirements for public safety radios demand that radio manufacturers have stringent quality control built in to the development process, regardless of whether the radio is implemented in hardware or software. The functional complexity that SDR facilitates may require different software quality assurance techniques, but SDR does not change the basic need to ensure that the software in the SDR is reliable and bug-free. This issue becomes more complicated if different waveforms are downloaded from different sources, as might be facilitated by wide adoption of an Intra-Device Interface Standard. When the software is downloaded, there needs to be some mechanism to ensure that the software will behave on the host environment as expected and without harmful effects. Issues include configuration management (ensuring that there are no incompatibilities with the specific version of waveform software and the particular version or configuration of the hardware/operating environment), ensuring that the waveform software is the product of a process that ensures a quality product (e.g., one that has achieved a certain level certification under the Capability Maturity Model for software development), ensuring that the software adheres to the IDIS, and so on. These issues can be addressed with rigorous integration and testing procedures as part of the development process.

Need to Override Security Controls

In the discussion of the responses, the members of the Public Safety SIG agreed that incident commanders would need a means to override security controls if they determined that such controls were preventing communication needed to protect life, safety, or property. The override would require the radio administrator or user to acknowledge the risk of entering an insecure operating state in order to minimize the potential of such a condition to occur mistakenly, unknowingly, or maliciously by unauthorized parties.

Implications of Non-Public Safety SDRs on Public Safety Communications

All of the discussion thus far concerns public safety use of SDR technology. The last consideration deals with the need to ensure that non-public safety use of SDR does not negatively impact public safety communications. With today's hardware-based radio technology, it is possible for someone to construct a communications device that (illegally) interferes with public safety communications, so this threat is not new. SDR technology, however, changes the likelihood that the threat will be realized and potentially increases the magnitude of the impact once that occurs. With SDR technology, there is a risk that even individuals with minimal radio expertise may be able to download radio software that could

interfere with public safety communications. The flexibility inherent in SDRs and the capability to download software capabilities creates the potential for greater disruption of public safety communications. The SDR Forum made this observation in the response to the FCC's *Notice of Proposal Rule-Making on Cognitive Radio* as follows: "The Commission's real concern is (or should be) that large numbers of radios could be modified simultaneously." The SDR Forum went on to advocate a regulatory solution of requiring parties seeking authorization of software defined, remotely programmable radios with hardware capable of transmitting in public safety bands to meet certain security and software authentication requirements.

4.5.3.7 Related Activities

The goal of interoperability may not be reached if the security architecture supporting radio communication is itself not interoperable. If a public safety agency uses different authentication techniques or provides different mechanisms for validating software, then systems will not interoperate unless users disable these security controls, which, of course, substantially increases the risk of a security breach. The widespread adoption of common security standards and protocols facilitates both interoperability and security. PKI offers one potential solution, as its related standards and protocols are mature and well-understood. For example, PKI technology enables Internet users to conduct secure transactions on e-commerce web sites even though these users may have had no prior relationship with the operator of the site. The public safety community would greatly benefit if it could implement a similarly successful system for SDR devices. One question is whether methods other than PKI exist for securing radio software. The Public Safety SIG has not yet identified another standard security technology that could provide equivalent assurance characteristics, and the issue must be further investigated before reaching consensus.

Independent activities within the public safety community such as the Global Security Architecture Committee and the Telecommunications Industry Association (TIA) TR8.8 Working Group, are considering security issues in evolving public safety networks. SDR security issues significantly overlap with other public safety security issues, and coordination between these groups and the ongoing work in the SDR Forum is important. As noted in the recommendations in Section 4.5.5, this is an area where dialogue between the public safety community and the SDR community is needed to ensure that security approaches are aligned.

4.5.4. Conclusions

- Interoperability for public safety could be impeded unless the security mechanisms for public safety are themselves interoperable.
- SDR introduces new security issues, such as how to verify the source and integrity of radio code during installation and how to prevent tampering with software once it resides on the radio device. Manufacturers and the public safety community are addressing those issues with current SDRs. This issue becomes substantially more complex as third-party software is introduced and as software downloads are accomplished over-the-air.
- What the most appropriate mechanisms are for ensuring security of public safety SDRs remains an open question at this time.

- Security considerations for public safety SDRs should be addressed in the broader context of security for wireless data in the public safety domain.
- Further work in security for public safety SDR should be based on a software development lifecycle model that reflects how software is developed and distributed to the end user for downloadable SDR.

4.5.5. Recommendations

- Security concerns related to SDR should be represented within the work of groups such as the Global Security Architecture Committee and TR8. The security architectures under consideration by these groups should become accessible by the Public Safety SIG, to ensure coordination in technology development and deployment.
- The Public Safety SIG should carefully delineate security requirements beginning with a systems development lifecycle model (including software distribution) for SDR so that these groups and others can develop appropriate architectures and eventually design secure systems.
- Research should be conducted to develop methods for integrating the P25 security architecture (ANSI/TIA-102.AAAB-A) with SDR security architectures for intra-device communication.
- Research should be conducted to develop key management and infrastructure options for public safety radio.

5. COST TRADE-OFFS, ECONOMIC MODELS, AND BUSINESS MODELS

One of the consistent themes in Sections 3 and 4 is that, in most cases, the implementation issues are rooted in cost and cost/benefit trade-offs. Although such a conclusion is typical for the introduction of new technology, the cost issues for public safety are different than those for the military or for the consumer market and need careful consideration in determining how SDR technology will eventually be deployed into the public safety market. This section includes a discussion of cost trade-offs as they relate to SDR technology for public safety.

Cost is a major factor for almost all communications systems. Public safety agencies typically must obtain funding by working with elected officials, most of whom are very cost-conscious with regard to buying new radio equipment. Further, vendors are motivated by potential financial returns. Due to these reasons, cost will have a large impact on the adoption rate of SDR technology.

Respondents were asked to discuss whether SDR technology would reduce communication costs for public safety agencies. Additionally, respondents were asked to examine the costs through the entire radio system life cycle and to identify the cost drivers and functionality trade-offs for public safety. Manufacturers noted that they are already producing Tier 2 SDR radios. As technologies mature and become more cost effective, Tier 3 and higher radios will begin to appear on the market.

5.1. Areas of Consensus in the RFI Responses

- Respondents agreed that SDR technology can provide cost savings. The manufacturers pointed out that, without a comprehensive cost versus functionality trade-off process, such savings might not be realized and, in fact, the costs could actually be higher with some types of SDR components.
- The business model used to describe the development of personal computers, also called the PC paradigm, may offer the best cost model for SDR radios. Under this paradigm, users make an initial investment in hardware and then implement the desired capabilities via software. The PC industry generally agrees that this has significantly reduced the cost of the hardware. However, as with the PC industry, public safety radios would still need to be upgraded periodically to increase processing power, increase memory, and so on, or to improve physical attributes such as the quality of a display.
- SDR technologies and software downloads could reduce the cost of system upgrades. This would reduce the cost by not relying on costly hardware parts and eliminating the need for radio technicians to physically touch each radio to perform the upgrades.

5.2. Areas of Divergence in the RFI Responses

- Some respondents believed that intra-device radio standards will lower the costs of SDR technology whereas others felt that it would increase the cost of implementing SDR technology.

- Two conflicting viewpoints exist regarding how legacy hardware can be incorporated into a new SDR radio system. One argument stated that legacy equipment could be used on a new SDR system until it reached the end of its life cycle, thus providing a cost savings. The counter-argument is that the legacy equipment would be out-of-date with an SDR system and would need to be replaced as a part of the migration. This would increase the cost of a system migration.
- The cost advantages of multi-band radios are uncertain and dependent upon how they are used. Although these radios can provide flexibility for expanding radio systems, some respondents felt that the higher cost of the multi-band radio offset its potential cost savings.

5.3. Analysis and Discussion

The design of a radio is a series of trade-off decisions, determining what functionality can be incorporated into a device against the cost, size, weight, power consumption, and so on required to accommodate the functionality. The cost trade-offs of SDRs will vary somewhat relative to traditional hardware radios, both at the device level and the life cycle level. The discussion in the following sections addresses the key trade-off considerations and how SDR technology impacts those decisions. This information can form the basis of cost modeling and analysis that can help the public safety community better understand the cost implications of SDR technology.

5.3.1. Cost Trade-off Considerations for Radio Design

A key aspect of a cost model is to identify cost drivers for candidate SDR technology implementations. Depending on radio requirements (e.g., which features are to be supported) and the particular SDR technologies being considered, the costs for some cost drivers are lowered with the use of SDR technology, whereas others may actually be increased. These relationships are constantly changing with the continual evolution of the SDR technologies, so the manufacturers indicated that they typically evaluate technology trade-offs for every new radio design. Also, SDR technology does *not* address many cost drivers in a typical public safety radio. Table 5-1 lists some of the more noteworthy of these, using a cellular phone as a reference. Such costs can thus be deemed “fixed” costs relative to SDR cost/functionality trade-offs.

Table 5-1
Fixed Cost Comparisons for a Portable Public Safety Radio

Cellular Handsets	Public Safety Portables
RF Power: 30-600 milliwatts	RF Power: 3-5 watts
Low RF power enable small, low-cost batteries	Higher RF power requires 1500-2400 mAH batteries
Limited Environment specs	Environment specs: Humidity, altitude, salt fog, wind-driven rain, vibration integrity, solar radiation
No drop test requirements	1 meter drop test
Limited operating temperature range	–30 deg C to +60 deg C plus storage 80 or 85 deg C
Low Audio output Power/Fidelity (into ear)	0.5 watt electrical into robust speaker to yield >80 dBa @ 50 cm
MTBF approx 1 year	MTBF > 3 years
Hum and Noise approx 35 dB	Hum and Noise 40-45 dB; better phase noise oscillators and dynamic range
Low cost display LCDs	Higher cost, shock-proof LCDs
Loose intermodulation specs—low-cost mixers and front-ends	70-75 dB intermodulation specs
Loose adjacent channel rejection specs	Up to 70 dB rejection @ 12.5 kHz offsets
Loose RX spurious specs	High RX spurious specs, affects LNAs, RX front-end filters
No FM/CSA issue	FM/CSA: cannot have explosive action in flammable atmospheres
Cheap TCXO	Higher cost TCXO with higher stability over wider temperature
Cheap, low-power antenna switch	Expensive switch to handle 3-5 watts
Millions sold, so ASICs used extensively to reduce power/cost	There are substantially fewer radios manufactured relative to cell phones, so ASICs are not as cost effective, especially for multi-protocol, multi-band, and multi-service operation.

Major upfront cost drivers that are subject to SDR architecture trade-offs are as follows:

- *Bandwidth* (in combination with high dynamic range requirements) is one of the most important drivers of cost as well as power consumption. Multi-band radios require multi-band antennas, wider bandwidth amplifiers and either high-dynamic range, high- speed digitizers, or replication of analog circuitry.
- *Dynamic range* is driven by stringent public safety adjacent channel rejection and intermodulation rejection requirements. Creates a need for A/D converters with many bits.
- *Transmit spectral purity* affects transmit modulator, PA, frequency synthesizer design, D/A converter dynamic range and TX filtering.

- *Receive adjacent channel rejection* puts demands on receive filtering as well as high dynamic range.
- *Multi-protocol Baseband Processing* Although a cost driver, it is less so than the above factors because its cost (as well as power consumption) has received the most benefit from Moore's Law increases in speed and density.
- *The amount of software overhead required* can impact the radio's required MIPS (million instructions per second) and memory, although this also benefits from Moore's Law. Higher MIPS can cause decreased battery life in addition to more expensive processors.

These cost/battery life drivers translate into the following SDR design considerations that must be traded against cost in addition to size, weight, and battery life:

- The radio's front-end design;
- The placement, number of bits, and dynamic range of the A/D converters in the receiver;
- The placement, number of bits, and dynamic range of the D/A converters in the transmitter;
- Partitioning, MIPS, and memory of the baseband processing;
- Antenna design; and
- Filter designs.

The placement of the A/D and D/A converters is a delicate balancing act in the design of a public safety portable radio. The closer to the antenna these converters are placed, the more "SDR-like" the radio becomes with the associated advantages of increased signal precision, repeatability, and, perhaps, being able to accommodate multiple frequency bands "digitally" without replication of analog circuitry.[29] However, these advantages must be traded against cost, reduced dynamic range,[30] and reduced battery life associated with the higher speed A/D and D/A devices that would be required.

Note that, from cost and battery life trade-off considerations, *multiple protocols* are much easier to accomplish than *multiple frequency bands.* This is because baseband processing tends to determine the ability of the radio to support multiple *protocols*, which can take advantage of Moore's Law growth in processing speed and density. To implement multiple bands, however, either high bandwidth, high dynamic range A/D and D/A converters would need to be placed close to the antenna or lower speed converters can be used with replication of analog circuitry. Today, the former method suffers from excessive power consumption[31] and cost. Furthermore,

[29] The "ultimate" SDR would have the converters connected to the antenna, so the entire radio would be "digital".

[30] To meet stringent public safety specifications on adjacent channel rejection, the dynamic range of the A/D converter must be sufficient to simultaneously accommodate weak on-channel signals and strong off-channel interference as much as 70 dB stronger. Available high sampling rate A/D converters tend to have lower dynamic range capability.

[31] Power consumption for A/D and D/A converters is a major issue for any portable implementation, and especially for public safety radios that typically mandate greater than 8-12 hour 5/5/90 battery life. For A/Ds with equal numbers of bits, power consumption is approximately proportional to sample rate. An A/D that operates at 1 MHz (approximately 2nd IF sampling) will typically require about 60 mW of power.

no imminent breakthroughs are anticipated from A/D converter technology to mitigate this problem. Replication of analog circuitry has the disadvantages of excessive cost and size if the radio has more than, for example, two frequency bands. It is this trade-off that has driven present-generation public safety radios to no more than two-band operation. Also, the cost burden on manufacturers for obtaining regulatory approvals for radios with several bands could be excessive due to the small number of units built in the public safety world.

In regard to baseband processing, a major cost/functionality and battery life trade-off is the partitioning of the high-speed baseband processing between devices such as DSPs, FPGAs, CCMs, and, in some cases, ASICs. Although ASICs have the lowest power consumption and highest speed, they tend to have fixed functions, and thus lack the programmability needed for SDRs. The cost of new ASICs in a public safety radio can be high compared to, for example, that in a cellular radio because the development NRE is apportioned to fewer quantities of manufactured units. FPGAs and CCMs, which are most suited to parallel processing functions and also demand considerable amounts of power, are more suitable for a multi-channel basestation implementation than for a portable device. Therefore, DSPs tend to be the "workhorses" of high-speed baseband processors in public safety radios, augmented with a lower speed general purpose processor for accomplishing network/user interfaces and general radio control.

There is no clear consensus under what conditions SDR technology will increase or decrease the cost of additional features when compared to a hardware-based radio. Figure 5-1 illustrates three cost models for a mobile radio. Here, it is assumed that a hardware-based radio is less expensive when there are very minimal features, such as when the radio needs to transmit and receive on only one frequency. A traditional hardware-based radio will have an additional cost for each feature. The solid green line represents this cost model of the direct relationship between new features and additional costs. In some cases, if the features are implemented via software, the cost for additional features will decrease relative to the hardware-based radio because software implementation does not require the manufacturing and installation of physical components. This cost model of the indirect relationship between new software features and cost is represented by the dotted blue line. Alternatively, the cost of developing the software for a new feature may be higher than the cost of a new piece of hardware due to the added hardware or processing capability required to support the new feature. This situation is particularly true in supporting additional frequency bands, as discussed earlier in this report. The dashed red line represents this last cost model.

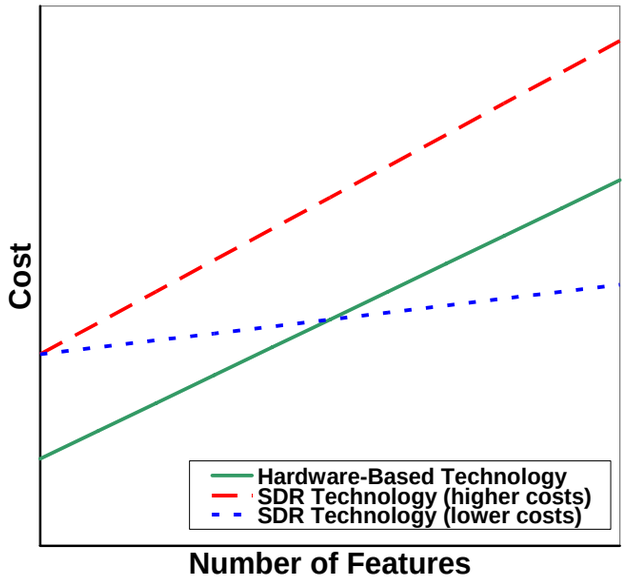

Figure 5-1
Projected Costs of a Handheld Radio

Additionally, the financial impact of intra-device radio standards on the upfront costs of a radio is unknown. As with the debate over the financial impact on features, there is disagreement as to whether intra-device radio standards will decrease the upfront costs of SDR radios. By requiring all software developers to adhere to an open standard, some argue that competition will drive costs down. Under the current hardware-based architecture, proprietary intra-radio technology is the norm. System owners are restricted to purchasing new equipment from a limited number of providers. IDISs offer an opportunity to create competition among software developers and perhaps thereby drive down prices. However, IDISs could constrict radio designs, increase hardware costs and, if the number of software developers is less than anticipated, the desired competition may not develop. This state of affairs could, in turn, raise the cost of IDIS radios above that of current hardware-based radios. Additionally, existing regulations require one vendor to certify the entire radio, which could cause that vendor to raise the cost of the radio due to increased testing or increased risks if third party software is used.

5.3.2. Life Cycle Costs

Life cycle costs include all costs associated with setting up (upfront costs), operating, and upgrading the radio system. Figure 5-1 depicts the life cycle costs of a radio system. Each of these life cycle phases is further discussed next.

5.3.2.1 Upfront Costs

Public safety radio systems in North America have, for the most part, been constructed and owned by a government agency. Because such systems typically require a significant outlay of funds at the onset, particularly if money is borrowed or raised through bonds, upfront costs are often key factors when choosing a technology. The initial implementation costs include the costs of the base model radio, the number of features added, and the infrastructure (towers, antennas, basestations, repeaters, and so on). For larger departments, the number of subscriber devices outweighs the other costs. The costs associated with a new system are driven by the costs of new subscriber equipment, which in turn are driven by the factors noted in Section 5.3.1.

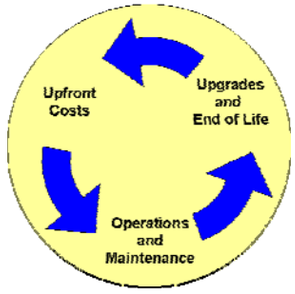

Figure 5-2
Life Cycle Costs

Based on the predominance of subscriber equipment replacement costs, SDR Tier 3 and expanded use of Tier 2 technology may not initially decrease the upfront costs of public safety communications systems. However, as more SDR radios are produced and key SDR device technologies continue to advance, component costs may decrease. Furthermore, intra-device radio standards may work to decrease the initial cost of the radios. Three unresolved issues include:

- *A manufacturing cost model:* Depending on the selected cost model, the upfront costs of SDR radios may be significantly higher than traditional, hardware-based models.
- *Cost impact of intra-device radio standards:* The longer-term impact of intra-device radio standards needs to be better understood.

- *Interoperability savings:* The costs of automating an interoperability solution, taking advantage of Tier 3 SDR, needs to be better defined.

5.3.2.2 Operational and Maintenance Costs

Operational and maintenance costs are those costs typically required to keep the system operating. They occur repeatedly on an annual basis and can vary based on the age of the system. Although operation and maintenance costs are relatively small on an annual basis, the total sum over the life of the system is a significant portion of the life cycle costs. For example, the National Law Enforcement and Corrections Training Center (NLECTC) estimates the annual cost of infrastructure maintenance to be 10 percent of the initial purchase price.[32]

Radios are the main source of communications for public safety personnel, so ongoing training is required to ensure that everyone is familiar with the features and operations of their radios. Additional training is required for new personnel. It is not yet known how SDR technologies will influence the cost of user training. Increased capabilities may require additional training, but cognitive capabilities and processing capabilities that are able to translate user functions into communications could simplify the user interface and reduce training requirements. Maintenance of SDR-based capabilities, although it may not necessarily increase training requirements, may require a broader set of skills than those needed for hardware-only capabilities.

To keep a radio system operating efficiently and effectively, routine maintenance is required. This maintenance involves both the fixed infrastructure and the user equipment. SDR technology may offer numerous maintenance cost savings. The ability of the device to diagnose its own problems is one major advantage. Software problems could be repaired automatically or with minimal intervention, and hardware problems can at least be identified. Many vendors already have some diagnostic software in their radios. Furthermore, valuable technician and user time could be saved with remote downloading of software maintenance releases and upgrades.

SDR technology could also simplify the procedures necessary to provide interoperability between incompatible radio systems. A gateway device implemented by using SDR could adapt to accommodate a new radio system by loading in the appropriate waveform, reducing or eliminating the upfront equipment purchases required with current technology.

In summary, SDR technology has the potential to reduce operations and maintenance costs. Self-diagnostic tools allow radios to identify problems and potentially correct them with minimal radio technician interaction.

5.3.2.3 Upgrades and End-of-Life

Upgrades allow an existing radio system to be brought closer to the current level of radio technology. These upgrades can improve productivity and/or extend the life of the system. Both of these improvements offer the potential for significant cost savings during this phase of the life cycle.

The ability to upgrade the communications system through a remote software download provides a significant potential cost savings. Because the system can be upgraded without a substantial hardware change, new standards can be implemented more inexpensively and

[32] *Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning, and Management*. NLECTC. January 2003. Pg. 8.

quickly. For example, a system manager looking at upgrading a hardware-based LMR system to a 12.5 kHz channel from a 25 kHz channel would need to invest in new radios to replace 25 kHz-only radios in addition to new fixed infrastructure. With SDR technology, though, the existing radios and infrastructure could be upgraded via software without requiring any hardware changes. By allowing the system to be dynamically updated, it is "future proof." In other words, as new applications, features, and standards are developed, the existing hardware can support them.

These graceful "software only" upgrades can be accomplished when the radio has sufficient digital processing speed, digital memory, bandwidth capability, dynamic range, switching speed, and spectral purity to meet the requirements of the upgrade. As such, it is important that the "reserve capacity" of design parameters such as processing speed and memory be incorporated into the radio from the start, with the amount of reserve being balanced against size, weight, cost, and power consumption. For instance, designing the reserve capacity into a radio to enable the addition of supporting more frequency bands can be a significant cost driver, as discussed earlier, due to the upfront additional hardware costs. However, adding a feature such as assigning an alphanumeric name to a radio channel may make financial sense only to be in the software.

To best leverage this "future-proof" benefit, SDR technology needs to support remote software downloads. Software downloads provide a quick and efficient method for loading new software onto each piece of equipment. Without over-the-air software downloads, radios will need to be pulled from active duty to be upgraded, and radio technicians will be required to directly install the new software.

An intra-device radio standard may ensure that all software can operate on the existing hardware and reduce the cost of upgrading radio systems. Currently, proprietary technology prevents system designers from picking and choosing the best available features from multiple vendors. An open architecture could allow new applications and features to run on any piece of compliant hardware. There are two major drawbacks to intra-device radio standards, however. As with the development of most standards, flexibility for developers is reduced. Additionally, if there is a problem, it may be difficult to identify the responsible party.

As discussed previously, SDR radios may also reduce the cost of transitioning between systems. SDR user equipment for the new system can be purchased and used on the existing system before a new radio system is turned on. The ability to simultaneously accommodate legacy and new systems can help spread the upfront costs of a new system over several years. By reducing the lump sum of the upfront costs, the new radio system may be more palatable for the budgeters. Additionally, once the new system is turned on, there is the potential that old user equipment may be used on the new infrastructure. Here, again, simultaneous operation of old and new equipment allows the old equipment to be used through its full life cycle and further reduces the number of radios that must be purchased at system turn-on.

In brief, SDR technology holds much promise for reducing the upgrades and end-of-life cycle costs of public safety radio systems. "Future proofing" allows existing SDR hardware to be used for longer periods of time. Remote software downloads provide quick upgrades without requiring radio technicians to physically touch every radio. However, two unresolved issues remain:

- *Total cost impact of remote software downloads:* The amount of savings from remote software downloads should be determined, along with costs to maintain secure software download capabilities and mechanisms for handling software licensing.
- *System transition costs:* A better understanding of the cost impacts of SDR technology on system transitions is needed.

5.3.2.4 SDR Impacts on Business Models

The analysis of cost drivers in the preceding sections assesses the impact of SDR technology in the context of traditional public safety business models in which a government agency periodically procures and builds out a radio system that it owns. However, SDR technology enables some alternative approaches to this business model that will ultimately provide a broader range of options to public safety agencies.

More recently, public safety agencies are using a method to build out systems by which another organization, such as a private business, builds out the system and then leases its use to public safety agencies. This has been an ongoing practice for agencies to avoid the high up front systems costs, and it can be financially beneficial to the private operator who may use towers and other physical infrastructure for other users as well. Europe provides more examples of public safety agencies that use commercial services as part of their radio communications. Law enforcement agencies are moving toward commercial carriers in the U.S. for wireless broadband data as well (see Case Study #4 for one such example). From the SDR perspective, the significance of this trend is that public safety agencies are increasingly taking advantage of communications options that increase capabilities without significantly increasing cost. The flexibility of SDRs can facilitate use of a variety of communications options and introduce additional business model options for public safety.

Case Study #4: Using Non-Public Safety Land Mobile Radio Systems

The IEEE 802.xx series of standards has seen strong acceptance in the market.

One case is Graham County, Arizona:

Graham County, Arizona has a population of 35,000 inhabitants and an area of 7,419 square kilometers (4,610 square miles). It is twelfth among Arizona's fourteen counties in both those measures. It is, however, a recognized leader in the application of commercially available wireless data support for its Public Safety community.

Operating from twenty towers, the system provides 802.11 access over nearly 1,600 square kilometers (1,000 square miles), and accesses 90% of the populated area of the county. It operates as a supplement to the county's VHF voice system, with a radio in each police car.

Currently, the car radio provides full connectivity to a laptop computer, bringing office functionality to the officer in the police vehicle. By completing daily paperwork in the unit instead of returning to headquarters, each officer spends some two hours a day more in the community, providing visibility, and in a position to respond quickly when needed.

The system is fully NCIC (National Crime Information Center) qualified, enabling officers to access a wide range of information directly rather then requesting it from the dispatcher. A great deal of attention has been paid to security, with the network operating as a private virtual network with secure point-to-point links.

Officers and the dispatch center have adopted instant messaging as a means of passing data around. Although VHF voice is still the primary command and control facility, the data system is more secure, and provides a convenient means of communication for many types of interaction.

The system is now in its second generation after four years of operation. The data rate into each vehicle is now 11 MB/s, up from the initial 1 MB/s. Each car acts as an access point inside the car, so the laptop connection is made with an internal 802.11 link. The next enhancement will be to add Bluetooth connectivity, and provide voice over IP connectivity through the system. A variety of devices, including PDAs, can be used inside the car with wireless connectivity.

The entire 113-kilometer (70-mile) length of the valley is connected with fiber, supporting not only this public safety system but also other governmental units' communications needs. A video system has both fixed and moveable cameras that feed pictures to fixed and mobile locations. An officer in one part of the jurisdiction can monitor traffic at another location by bringing up a camera image on the screen in the vehicle.

The business case is worth noting. The radio for each unit costs $1,500US. Each tower with associated equipment is $3,500US. The total investment to support Graham County's 35 police officers is under $200,000US. Using the value of two additional hours per day in the community, payback on the system is less than a year.

This information was provided by John Lucas, Information Technology Director of Graham County, Arizona. It was compiled by Peter G. Cook of the Software Defined Radio Forum in conjunction with the report on Public Safety Use of SDR Technology under development by the Public Safety SIG. Inquiries should be directed to Galen Updike, State of Arizona, gtupdikg@azgita.gov

SDR technology can facilitate the options available to key players in public safety communications. For example, as noted in Section 3.2, multi-band, multi-protocol, multi-service radios would allow single devices to operate on multiple communications networks. Adding cognitive applications to the mix would potentially facilitate development of radios that could operate on multiple networks and determine in real-time the "best" communications path and/or network to use for a given transmission based on urgency, cost, network loading, and so on. SDR technology may also change the cost models for system operators, in addition to users.

One example of a change in cost models would be for an operator to use multi-service basestations that could allow system operators to provide services to public safety as well as commercial services. Although the motivation for this approach is to amortize basestation costs across multiple service groups, the RF hardware of the multi-service basestation would need to meet the requirements for both services, which could increase the upfront cost of the cellular station. Current coverage topologies are different between cellular and public safety. One key

driver for a public safety coverage design (and, thus, the tower placement) is the stringent required coverage reliability, which often includes heavy in-building coverage. Also, whereas cellular site-placement topologies are efficient for individual calls, public safety coverage topology, for systems with dense user population and wide-area talkgroups, tends toward longer range, higher towers, and higher power to avoid spectrally inefficient transmission on numerous frequencies from many sites during a group call. A limiting example of the effects of this group call forcing function is simulcast transmission, which is often the only plausible coverage solution in major population areas with limited frequencies available.

Technology advances could lead to some convergence of these differing topologies. If the above technical issues can be resolved, and if appropriate service-level agreements can be negotiated between such providers and public safety, SDR could provide opportunities for system operators to amortize infrastructure costs over a much greater base than just public safety. In addition, such arrangements could lead to such possibilities as dynamically reallocating bandwidth and spectrum from commercial services to public safety in major emergencies.

SDR technology may also enable users to more effectively accommodate new requirements and incorporate new technology. Progress in information and communication technology has been closely associated with improvements in semiconductor technology, for instance. Commercial and government organizations have both taken advantage of technological advances to address their problems. As they do so, their operational experience finds shortcomings in existing capabilities and leads to new statements of requirements. These new requirements are typically incremental, moving a short way beyond the existing capabilities, rather than breakthroughs. For the public safety community, new requirements include, for example, geolocation, data delivery, interoperability, and enhanced command and control. More radical proposals, such as the system of systems concept, have initially been viewed with considerable caution. A change in requirements can happen at any point in time as the result of new legislation, civic growth, or availability of new funding in a particular area. The rate of acceptance of SDR technology can be significantly enhanced if such factors can be leveraged to obtain earlier adoption. In the absence of incremental justification, radio equipment will be replaced on an extended schedule, often when the existing system is well into obsolescence. SDR-based equipment may have the characteristic of initially working with an older system and then accepting software to operate with a new system when the new system arrives.

SDR technology will also present the potential to create a more rapid turnover of technology in the form of software. SDR could also lead an environment where software licensing models will be the major ongoing public safety cost factor to operating a system. As with typical information technology systems, keeping software current as a price of entry for ongoing vendor support will become the norm. Payments to vendors for software maintenance and upgrades then creates an ongoing and steady stream of money flow between system operators, taxpayers and manufacturers.

In the terminology of technology transfer, the public safety community is composed of “late adopters” —decision-makers who defer implementing a new technology until the level of uncertainty is low. As such, the late adopters will carefully evaluate the benefits of a new technology in their specific circumstances. The purchase of technology for the sake of technology is not a characteristic of the public safety community. New technology will receive serious attention when it offers an opportunity to meet new requirements or when it offers

significant cost benefits. It is not necessary for a new technology to be a direct evolution from current systems. For example, if the ability to transmit data to an emergency vehicle is a requirement, a logical extension is to modify an existing land mobile trunked system. Alternatives might be to develop a data path through the local cellular system or to use a commercial offering such as Wi-Fi.

5.3.2.5 Considerations for Joint Procurement of Current JTRS Radios for Public Safety Purposes

Current discussions regarding existing JTRS radios illustrate some of the framework of economic decisions regarding purchase of public safety radios. The JTRS radios are currently designed to meet primarily military requirements such as Type I security, with the ability to cover a wide range of frequencies and typically support a larger number of waveforms than required by public safety. The cost impact of this increase in functionality relative to public safety radios has to be compared with the economies of scale that would permit joint procurement among different user domains (e.g., military and public safety). Better understanding of the economic implications of radio functionality (as noted in the first recommendation in Section 5.5) will assist both the public safety user community and the vendor community in defining appropriate function sets to meet user requirements for future public safety radios.

In addition to the above analysis, there is a role for the JTRS community in development and fielding of SDR solutions to enable the military to support interoperable functions and waveforms with the public safety community for usage in case of major national disasters requesting deployment of joint public safety and military capabilities.

5.4. Conclusion

- Vendors are already putting SDR technology into operation, with many features implemented in the software, including, in some instances, multiple protocols. It is expected that vendors will continue to employ SDR solutions when SDR can provide a satisfactory return on investment, perhaps by reducing the manufacturing cost of a radio via shifting capabilities to software. This trend toward SDR deployment will largely be driven by new technologies becoming available at market-acceptable prices.
- Respondents believe that there is further room for improvement to lower life cycle costs by leveraging SDR capabilities to reduce maintenance, operations, and upgrade costs. Remote software downloads could play a key part in lowering these costs.
- There is disagreement on the effects of intra-device radio standards, the cost/benefits associated with the use of an intra-device radio standard, the cost impact of legacy hardware, and the cost impact of multi-band radios.
- A framework for better understanding of the relationship of functionality and life cycle cost is needed. This will allow the public safety community as a whole (users and vendors) to better understand critical cost trade-offs and articulate required and desired functionality.

5.5. Recommendations

- The Public Safety SIG should further analyze the radio system life cycle to consider the impact of SDR cost versus benefits on each of the following:
  - Manufacturing;
  - Intra-device radio standards;
  - User training and methods to reduce these training costs;
  - Routine system maintenance;
  - Remote software downloads, including costs and benefits from productivity improvements and additional manufacturing costs; and
  - System transitions.

Once these six issues have been addressed, a more complete cost model for SDR technology should be developed.

- A better understanding of the cost breakdown (both in terms of hardware and software) of SCA-compliant products should be developed. Life cycle costs, as well as the potential cost reduction of opening the market to niche companies and the additional integration and testing costs, must be factored into the cost breakdown.
- Additional analysis is needed on the cost trade-offs of various alternative public safety requirements and candidate features and capabilities. Cost trade-offs need to be characterized for both individual units as well as the overall system.
- Cost models reflecting the current national priority on enhancing first responder communications and the cost avoidance of improving interoperability need to be characterized.
- A better understanding of cost breakdown (hardware and software) of radios with multiple bands and/or multiple modes should be developed.
- The Public Safety SIG should build a business case analogous to the Business Case for Commercial Services (note the initial work on this topic in Appendix B). The purpose of the business case is to capture the business relationships among developers, users, funding sources, regulators, and other stakeholders to provide a context for assessing the impacts of SDR on such relationships and to depict how SDR can create new business cases and business models.

6. SUMMARY CONCLUSIONS, RECOMMENDATIONS, AND NEXT STEPS

6.1. Conclusions

SDR technology is no longer a futuristic concept still in the research phase. The reality is that public safety radios being manufactured today fit the SDR Forum's definition of a Tier 2 software defined radio. SDR technology is already allowing flash upgrades to radios to install new capabilities and reduce manufacturing and maintenance costs. However, interoperability is the application of SDR that could have the greatest significance in improving public safety communications. Because today's implementation of SDR technology in public safety radios does not include multi-band or multi-service capabilities, this implementation of SDR does not yet accomplish the goal of seamless interoperability. Although a number of technical and operational issues are still to be resolved to achieve the promise of interoperability, SDR technology has significant potential to enhance communications capabilities for public safety. There are several different scenarios in which interoperability could be significantly improved with the deployment of SDRs that incorporate multiple waveforms (e.g., multiple frequency bands, multiple channel bandwidths and configurations, and multiple protocols). Although interoperability is the most compelling argument for SDR technology, several other significant potential advantages of SDR technology include the potential of cost reduction for upgrading and maintaining equipment, the ability to adapt to evolving technologies and standards, ease of operation, and performance optimization.

The top priority in achieving interoperability among public safety users is to use SDR technology to develop multi-band radios (e.g., VHF/UHF/800). One of the major impediments to interoperability of public safety radios is that public safety communications operate on multiple frequency bands. Creation of a multi-band radio would make significant inroads in addressing the interoperability challenges faced by the public safety community today.

Another capability for SDRs is multi-service radios in which different waveforms (land mobile radio network, personal area network, cellular, Wi-Fi, and so on) can be executed in a single radio. Such devices could operate across multiple systems, thereby supporting a "system of systems" concept for public safety communications. Multi-service devices could provide the public safety community with opportunities to take advantage of a rapidly growing set of possible communications services, network types, and so on. These capabilities may be important for first responders to communicate to non-first responders, but could be used among first responders as well.

Multi-service radios that extend beyond public safety land mobile radio waveforms could also facilitate greater use of commercial services. Commercial wireless organizations have an opportunity to position public safety as an application market by tailoring their product offerings to meet the incremental requirements posed by public safety organizations. Government organizations have the opportunity to both fund programs with specific public safety content and to work within organizations, such as the SDR Forum, to develop standards around those programs and promulgate information about them.

In addition to multi-protocol, multi-band, multi-service capabilities, SDR technology lays the groundwork for cognitive applications in public safety radio systems. Over the coming years, cognitive applications will become the wireless norm for numerous domains, including

public safety. Cognitive applications offer significant potential benefits to public safety, ranging from performance optimization to making the flexibility and complexity of SDRs seamless to the user.

Dynamic spectrum allocation and spectrum efficiency are often touted as advantages of cognitive applications. The public safety community's requirement for immediate access to spectrum for mission-critical needs means that spectrum licensed to public safety users cannot be dynamically allocated for non-public safety use unless there is a reasonable guarantee that the spectrum is available for public safety use when needed. It is also recognized that spectrum demands, especially during major incidents, can be significant. Thus, increases in efficient utilization are beneficial. Development of technology for more efficient spectrum utilization should be based on an understanding of how spectrum is truly utilized today. However, there is a lack of quantified data on spectrum utilization across all services (e.g. public safety radio services, commercial services, other private wireless services, federal government, etc.) during routine, pre-planned events and emergency incident situations. Collection and analysis will require development of specialized data collection equipment. These data would support spectrum planning, sharing, and usage-modeling activities.

The potential benefits outlined above are significant and substantial, but many issues remain to be resolved in order to achieve the envisioned benefits. Even to realize the initial step of multi-band radios, front-end RF, multi-band antennas, and front-end sampling technologies are critical and in need of accelerated development. As the frequency span covered by the radio (in terms of number of octaves) increases, the technical challenges increase as well. Considerable debate remains as to whether the deployment of SDR technology to facilitate multi-band operations will focus on infrastructure or the terminal/subscriber device level. The processing capability to accommodate multiple bands impacts size, weight and power consumption, which must be tightly budgeted in subscriber equipment, especially portable radios. The greatest benefit to the user, in most instances, and the most seamless interoperability is achieved when the SDR capability can be implemented at the subscriber level.

Some challenging technical issues are significant cost drivers in the development of multi-service devices. These include capabilities to access public safety land mobile radio networks and other communications networks, such as cellular systems, Wi-Fi systems, and so on. In addition, the technical issues in developing multi-service devices include frequency span and linearity. Multi-service devices that support the system of system concept introduce additional concerns to allow seamless migration across systems, including relaying of site-adjacency information across disparate systems, authentication, and sharing of encrypted information. Operational procedures must also be put in place to ensure smooth operation in a system of systems environment. Multi-service devices can also become unwieldy and overly expensive in an attempt to accommodate dissimilar functional requirements.

The ability to download software to a radio presents additional security concerns for SDRs. Also, the introduction of an Intra-Device Interface Standard (see the following paragraph) and the potential for loading waveforms from multiple sources onto a radio operating environment require clear definition of security requirements for waveform software. Interoperability for public safety could be impeded unless the security mechanisms for public safety are themselves interoperable. SDR introduces new security issues, such as how to verify the source and integrity of radio code during installation and how to prevent tampering with software once it resides on the radio device. What the most appropriate mechanism is for ensuring the security of

public safety SDRs remains an open question at this time. Security considerations for public safety SDRs should be addressed in the broader context of security considerations for wireless data in the public safety domain.

These technical issues are by no means impossible to solve, but they are still daunting. One way to accelerate the process is to leverage relevant existing work in SDR. The military's Joint Tactical Radio System (JTRS) is the most technically complex implementation of SDR technology. However, a number of issues exist in leveraging the technology for public safety. JTRS radios have been developed to meet military requirements, making the cost too high for the value they provide for public safety agencies. However, the architecture of the JTRS radios, based on the Software Communications Architecture (SCA), may be considered. A major distinction exists, however, between the architecture of today's public safety radio systems (and the standards that support them) and the SCA. The SCA addresses standard interfaces *within* a device. To date, the public safety community has worked toward standards *between* devices but not within a device. Therefore, introduction of an intra-device interface standard such as the SCA would make significant changes to the current business models and processes for development, deployment, and regulation of public safety communications equipment. An alternative approach, standardizing on an intra-device interface but not using the SCA as a model, is another option, although the cost trade-offs and implications of adopting an IDIS are not well understood. The cost trade-offs of the SCA have not been quantified.

Many of the design considerations come down to a cost issue. Although it may be feasible to create a multi-band, multi-service, performance-optimizing cognitive radio, it may not be affordable or cost-effective for public safety. Even some of the broader issues, such as an IDIS have significant cost trade-offs. The tradeoff for an IDIS is between introducing more competition by facilitating the entry of software or hardware component developers versus the additional test and integration costs associated with creating a radio from components that comply with a standardized interface. Cost models need to be developed to assist the community as a whole in understanding the implications of resolving the issues identified in this document. Furthermore, because product design is a trade-off between cost and functionality, prioritization of public safety requirements by the users will assist product developers in targeting the right points on the cost-functionality curve.

We fully recognize that some of the implementation scenarios contemplated in this report have significant regulatory impacts. For example, the introduction of an IDIS leads to a number of questions about how to define compliance with the standard, who should be responsible for ensuring that specific combinations of standards-compliant operating environments and waveforms will behave as expected, and what level of testing is appropriate and necessary for radios integrated from combinations of waveforms obtained from different sources. Multi-service devices may also require rethinking of regulations which, today, are focused on service-specific rules (i.e., in the United States, private land mobile radio is governed by Code of Federal Regulation Title 47 Part 90, whereas commercial cellular systems are regulated based on Title 47 Part 21).

The ultimate vision for public safety communications is simple: first responders, whether in normal routine operations or arriving at the scene of a major incident, are able to communicate with whomever they need to, whenever they need to. Numerous issues and details need to be resolved to realize that vision, as documented in this report, and software defined radio is a technological pathway to realizing that vision.

6.2. Recommendations and Next Steps

6.2.1. Recommendations

Three major types of recommendations are made throughout this report: technology research, cost models, and outreach. These recommendations are further discussed below.

6.2.1.1 Technology Research

The Public Safety SIG supports and encourages investments by government research programs and manufacturers to address the issues listed below:

1. Develop and deploy SDR technology that enhances public safety interoperability, especially for the radios' front-end and high-speed sampling devices that will improve the performance/cost ratio for developing multi-band radios. (Section 3.1)
2. Identify the feasibility, technical issues, and cost trade-offs associated with implementing multi-service radios, which include, but are not limited to, the combined implementation of the modulations (including linear), protocols, infrastructure, network, and regulatory implications. (Section 3.1)
3. More explicitly define how SDR technology can support the implementation and adoption of the P25 ISSI and how the ISSI might eventually be enhanced to support and exploit SDR capabilities. (Section 3.2)
4. Develop SDR technology that supports seamless migration of devices, authentication, and handling of encrypted information across systems. (Section 3.2)
5. Develop regulatory regimes needed to effectively implement standards, particularly as part of the cost/benefit trade-off analysis of an IDIS. (Section 4.2)
6. Assess the feasibility of a version or variant of the SCA that would meet device requirements (processing, memory, power, and so on) for public safety. The Public Safety SIG should support the ongoing work in the SDR Forum to investigate an "SCA-light." (Section 4.2)
7. Assess the feasibility of an IDIS designed specifically for public safety application but not based on the SCA. (Section 4.2)
8. Engage appropriate standards organizations (e.g., TIA, ETSI, IEEE, OMG) as part of the process of assessing standards feasibility. If feasibility can be established, identify and develop standards. (Section 4.2)
9. Conduct additional research to identify the appropriate role of standards for software downloading. (Section 4.2)
10. Collect, document, and analyze additional spectrum usage monitoring data. (Section 4.3)
11. Delineate security requirements, beginning with a systems development life cycle model, to promote the development of appropriate architectures and secure systems. (Section 4.5)

12. Identify methods for integrating the P25 security architecture with SDR security architectures to ensure intra-device communication. (Section 4.5)
13. Develop key management and infrastructure options for the public safety community. (Section 4.5)
14. Work with groups such as the Global Justice Information Sharing Initiative (Global) Security Architecture Committee and TR-8 to address security requirements and potential solutions to security issues. (Section 4.5)

6.2.1.2 Cost Models

1. Develop cost models for the terminals and infrastructure in the public safety domain to better understand the benefits versus cost trade-offs of implementing SDR in each of these devices. (Section 4.1)
2. Develop cost models for intra-device radio standards in the public safety domain. (Section 4.2)
3. Develop cost models for various multi-band and multi-service radios in the public safety domain to determine which combinations are most cost effective. (Section 4.4)
4. Develop individual cost models for phases of the radio system life cycle including: (1) manufacturing, (2) user training, (3) routine system maintenance, (4) remote software downloads (including productivity improvements and additional manufacturing costs), and (5) system transitions. Once these five issues have been addressed, a more complete cost model for SDR technology can be developed. (Section 5)
5. Perform additional analysis on the cost trade-offs of various alternative public safety requirements. Characterize cost trade-offs for both individual units as well as overall system cost. Cost models reflecting the current national priority on enhancing first responder communications and the cost avoidance of improving interoperability also need to be characterized. (Section 5)
6. Build a Public Safety Business Case Model to a similar level of detail as the Business Case for Commercial Services (see Appendix B), noting that SDR can create new business cases and business models. (Section 5)

6.2.1.3 Outreach

1. Public Safety SIG should work with the public safety community to help determine the operational implications of the capabilities of SDRs and develop materials to assist in the dissemination of the information to public safety users. (Section 3.1)
2. The public safety community needs to investigate any possible synergies with other users of frequencies at or near the public safety bands. (Section 4.4)
3. Enhance participation in the SDR Forum and other educational venues to better understand the benefits versus cost trade-offs of SDR technology.

6.2.2. Next Steps for the Public Safety SIG

1. Continue to monitor developments in the military's GIG program (Section 2.3) and E2R (Section 2.4).
2. Continue to support the development of end user communities' participation in the SDR Forum. (Section 3.3)
3. Follow this report with a review of the updates to the Public Safety Statement of Requirements document to confirm/update this analysis with respect to the revised and detailed requirements. (Section 3.4)
4. Approach Project MESA to determine whether there is a mutual benefit in reviewing this report based on the already defined Project MESA requirements. We anticipate that this dialogue would be maintained informally through the public safety representatives that support both Project MESA and the Public Safety SIG. (Section 3.4)
5. Engage TIA, ETSI, IEEE, and OMG in discussions regarding the feasibility of standards for SDR technology. (Section 4.2)
6. The Public Safety SIG should monitor and assist in the SDR Forum's work on definitions. Responses relating to definitions and terminology should be referred to the relevant SDR Forum groups (Cognitive Radio WG and Cognitive Applications SIG) for inclusion in their ongoing work program. (Section 4.3)
7. The SDR Forum should devote continued emphasis on studies and promotion of these technologies to ensure that the developers of these technologies are cognizant of the public safety community's requirements. (Section 4.4).

6.3. Future Vision

Given the enormous potential outlined in this report for SDR technology to enhance public safety communications, and given that fact that public safety radios are already beginning to incorporate SDR technology, there is little doubt that SDR will continue to significantly impact public safety communications. Precisely how the technology penetrates the market and what the products of the future will look like remains to be determined.

There are a variety of scenarios in which SDR technology could be manifested. The current market trajectory, in which the current manufacturers continue to add features with greater emphasis on software implementation could continue. As technology brings costs down and the demand for interoperable capabilities continues, current multi-protocol and limited adjacent frequency band capabilities will be enhanced with capabilities for more protocols, as well as wide frequency multi-band and multi-service operation. Over time, cognitive applications will be implemented as well.

Another scenario is based on the Intra-Device Interface Standard. Creation of such a standard could lead to devices that include a variety of waveforms as needed to meet public safety functional requirements, possibly provided by waveform vendors. In this scenario, a market potentially develops for waveform developers, radio platform specialists, and/or device and systems integrators.

Yet another scenario could be based on a new communications infrastructure based on SDR technology, dedicated to and controlled by public safety. Centralized architecture and security management, along with a standard with some level of open interfaces, tailored to the needs of public safety, could provide substantial digital bandwidth, very wide area coverage, nearly universal interoperability, and specialized local communications management for incident sites. A carefully developed prioritization scheme could meet the response time requirements with high-performance paths through the broadband channels for emergency traffic.

Technology developments, market forces, user requirements, and government roles will all influence what combination of the above scenarios actually comes to pass. What is more certain is that SDR technology will significantly impact public safety communications. In the days of call boxes, the appearance of mobile radios in police vehicles significantly changed public safety communications. In the days of single channel radio systems, trunked radio systems significantly changed public safety communications. SDR technology holds the same promise for significant change in the future.

A. ACRONYM GLOSSARY

2G – second generation
3G – third generation
A/D – analog-to-digital
ATF – Alcohol, Tobacco & Firearms (U.S. Dept. of Justice bureau)
AMC – artificial magnetic conductor
AP – access point
APCO – Association of Public Safety Communications Officials
AR – access router
API – Application Programming Interface(s); Application Program Interface
ARPU – average revenue per user
ASIC – application-specific integrated circuit
CA – Certification Authority
CASIG – Cognitive Applications Special Interest Group
CB – Citizens' Band
CCM – configurable computing machines
CDD – Capabilities Deployment Document (JTRS)
CONUS – continental United States
CORBA – Common Object Request Broker Architecture
COTS – commercial off-the-Shelf
CR – cognitive radio
CRWG – Cognitive Radio Working Group
D/A – digital-to-analog
DEA – Drug Enforcement Administration (U.S.)
DOT – Department of Transportation (U.S.)
DPD – Denver Police Department
DSP – digital signal processor
E2R – End-to-End Reconfigurability (European research project)
EMS – emergency medical service(s)
ETSI – European Telecommunications Standardisation Institute
FBI – Federal Bureau of Investigation (U.S.)
FCC – Federal Communications Commission (U.S.)
FDLE – Florida Department of Law Enforcement
FEMA – Federal Emergency Management Agency (U.S.)
FHP – Florida Highway Patrol
FM/CSA – Factory Mutual/Canadian Standards Association
FPGA – Field Programmable Gate Array
FR – first responders
FRS – Family Radio Service
GIG – Global Information Grid
GOS – grade of service
GPP – general purpose processor
GPS – global positioning system(s)
HW – hardware
IAN – Internet area network
ICTAP – Interoperable Communications Technology Assistance Program

IDIS – Intra-Device Interface Standard
IDL – Interface Definition Language
IEEE – Institute of Electrical and Electronics Engineers
INS – Immigration and Naturalization Service (now U.S. Immigration and Customs Enforcement
IP – Internet Protocol
ISSI – Inter-RF Subsystem Interface
JAN – jurisdictional area network
JPO – Joint Program Office
JTRS – Joint Tactical Radio System
JTTF – Joint Terrorism Task Force
LCD – liquid crystal display
LMR – land mobile radio
LNA – low-noise amplifier
LPD – Low Probability of Detection
LPI – low probability of intercept
LOS – line-of-sight
MANET – Mobile Ad-hoc Networking
MBOA – Multi Band OFDM Alliance
MBWA—Mobile Broadband Wireless Access
MEM – microelectromechanical
MESA – Mobility Emergency Safety Applications
MIRS – Metropolitan Interoperability Radio System (Washington, DC)
MoU – Memorandum of Understanding
MTBF – mean time between failure
NATO – North Atlantic Treaty Organization
NC3 – NATO Consultation, Command and Control
NCIC – National Crime Information Center
NIJ – National Institute of Justice
NLECTC – National Law Enforcement and Corrections Training Center
NRE – non-recurring expense
OEM – original equipment manufacturer
OFDM – Orthogonal Frequency Division Multiplexing
OMG – Object Management Group
OPEX – operating expense
P25 – Project 25
PA – power amplifier
PAN – personal area network
PC – personal computer
PCS – Personal Communications Service
PDA – personal digital assistant
PIM – Platform Independent Model
PKI – public key infrastructure
PPDR – Public Protection and Disaster Relief
PS – public safety
PSM – Platform Specific Model

PSPP – Public Safety Partnership Project
PTT – push-to-talk
QoS – quality of service
R&D – Research and Development
R&O – Report and Order (FCC)
RAN – Radio Access Network
RF – radio frequency
RFI – Request for Information
RX – receive(s)/receipt(s)
SCA – Software Communications Architecture
SDR – software defined radio
SIG – Special Interest Group
SME – small to medium enterprise
SOF – Special Operations Forces
SoR – Statement of Requirements
SW – software
TCXO – temperature compensated crystal oscillator
TDMA – Time Division Multiple Access(es)
TETRA – TErrestrial Trunked RAdio
TIA – Telecommunications Industry Association
TICP – Tactical Interoperable Communications Plans
TPC – transmit power control
TX – transmit(s)/transmission(s)
UASI – Urban Areas Security Initiative
UHF – ultra high frequency
UML – Unified Modeling Language
UWB – ultra wide band
VHF – very high frequency
WB – wide band
Wi-Fi® – Wireless Fidelity
WiMAX – Worldwide Interoperability for Microwave Access
WLAN – wireless local area network
WMD – weapons of mass destruction
XML – eXtensible Modeling Language

B. PRELIMINARY PUBLIC SAFETY BUSINESS MODEL

In analyzing the responses to the RFI, the Public Safety SIG came to two conclusions: (1) as noted in the report, almost all of the technical issues included some cost trade-off discussions, and (2) there is not a good representation of the business model for public safety that could be used to provide the needed context for discussion of cost trade-off issues. In this Appendix, we present some initial thoughts regarding a business model for public safety communications, with an acknowledgment that additional work is needed on this topic.

The SDR Forum has been developing business models for other domains. By using the same methodology, the initial concept for a public safety business model is presented in Figure B-1. For purposes of comparison, a business model representation for commercial cellular is presented as Figure B-2 at the end of this Appendix.

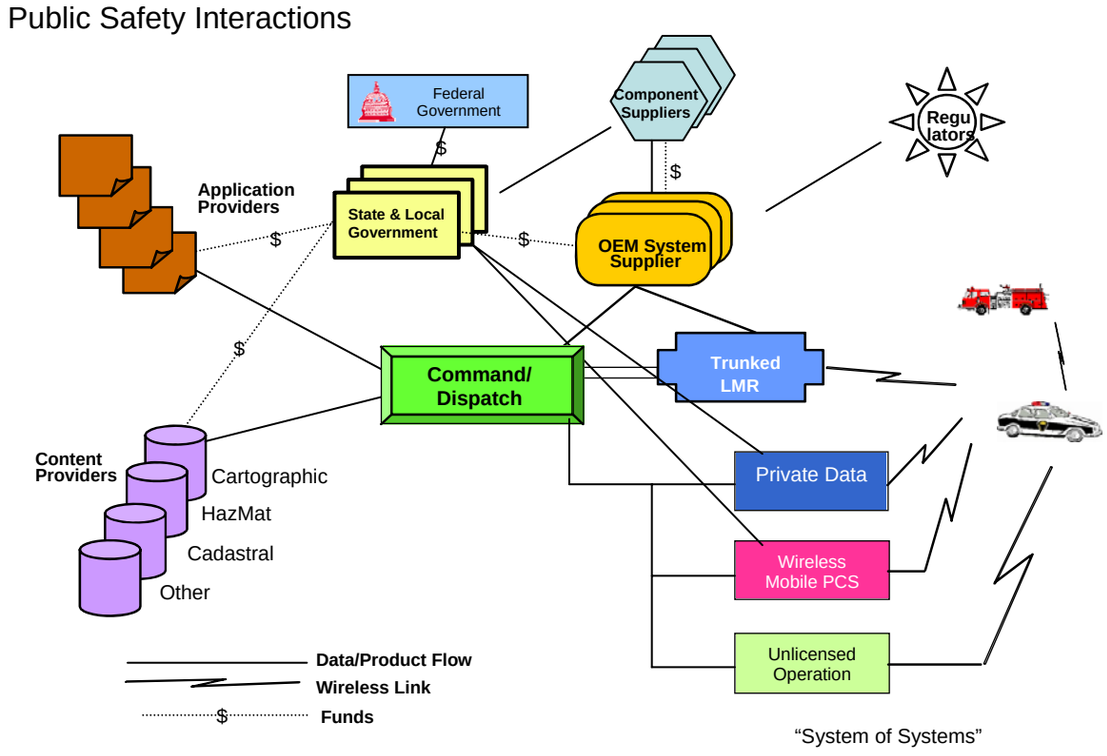

Figure B-1
Public Safety Business Model

This diagram represents a model of certain interactions between entities with public safety roles. Many relationships are not reflected here, and other versions of the picture can be created to emphasize other aspects. This model is intended to serve the purpose of simplifying the process of indicating, "This is what we are talking about," in discussion of the public safety arena and its players.

In the center is the command facility for an individual police, fire, or other public safety organization. In the United States alone, there are some 50,000 of these organizations, which are extremely diverse in size and in the range of problems with which they deal. The command

function manages operations, and routine communications, most commonly voice, connect dispatchers with first responders in the field.

Public safety first responders have a variety of communications facilities available to them, both in their vehicles and on their persons. Land mobile radio (LMR), often trunked for efficiency, is the first responders' primary means of communication among themselves and with the dispatch center, where telephone calls for assistance are taken.

Also very diverse are the many state and local governments that use their legal authority to authorize, recruit, equip, and make policies for their public safety units. The sheer magnitude of the numbers of organizations operating independently makes public safety a very fragmented market.

Federal government is also a major player in the business mode for public safety communications. The federal government role includes both legislation levying requirements on individual municipalities and public safety organizations and funding to procure equipment.

In the past, voice communications systems provided by original equipment manufacturer (OEM) suppliers have been the primary or even sole communications facilities available to support the first responders. Those OEM suppliers integrate a number of components from component suppliers and assume system responsibility for effective operations.

Increasingly the "system of systems" concept is being incorporated into public safety communications capabilities First responders are provided with cell phones, data radios and unlicensed devices using Wi-F, Bluetooth, and other commercial communications capabilities. The philosophy of a system of systems is to take advantage of a variety of options rather than the monolithic architecture that characterizes the primary voice systems. Any number of communications capabilities have potential to support some aspect of public safety operations.

The left side of Figure B-1 depicts a number of applications and data resources. These applications, some commercially available and some dedicated to public safety needs, are used to deliver information and direction to first responders responding to an event. A cartographic database contains detailed map data for the jurisdiction, data that is displayed using a geographical information system that can change parameters to meet the needs of specific incidents. Hazardous materials (HazMat) are often present at the scene of an incident, and first responders are trained in how to handle them and are given detailed data on the characteristics of the materials encountered. Cadastral data describes property lines, building ownership and related legal information about a jurisdiction.

The role of regulators, depicted in the upper right of Figure B-1, is to make rules to implement legislation and recommend legislative changes. They also enforce applicable regulations.

The figure also shows some of the flows of funds, products, data, and wireless communications existing in the public safety communications market. State and local governments receive money from taxation, the federal government, and other sources. State and local governments lease or purchase communications systems from the OEM suppliers and the systems are installed in local facilities. They also purchase application, data, and a variety of services used to support public safety operations.

Wireless links enable mobility of first responders and their vehicular units. Both dedicated public safety systems and commercially available services are used.

The majority of public safety systems are closed systems, for which there is no revenue stream directly from the user to the operator. In most cases the system is owned by a government entity, often the same entity that employs the users The cost of this communications system is regarded as a cost of doing business. There may be some inter-departmental cross-charging methodology or, where a central authority supplies shared infrastructure, a charge may be made that reflects the number of users. In these cases, one can identify roles that are similar to user and operator roles in a commercial provider scenario. But even in these situations, no new revenue enters directly into the model from the user.

Revenue streams are much different for commercial carriers. Now that, particularly in Western Europe, the cellular markets are mature at high penetration levels, the rate of increase in subscriber levels is much lower and the emphasis is not focused so much on increasing the numbers of new subscribers, for which there is a cost (and many of the changes are associated with customers changing providers, i.e., churn, rather than real new subscribers), but on customer retention.

In most of the cellular markets, the operator pays full cost for the terminals and subsidizes the cost to different degrees to make it more attractive to new customers. The operator does so by having the terminal and subscription bundled with various airtime packages. The price to the customer depends upon the degree of contract "tie-in." The operator seeks to claw back the subsidy as soon as possible through encouraging usage by the new customer. At the same tim,e the operator is increasing the average revenue per user (ARPU) of existing customers through offering a greater range of attractive and innovative multimedia services such as software downloads, ring tones, video clips, and so on. This process is very competitive and complex. Many alliances among network operators, manufacturers, and content providers have been formed to achieve profitability. Each group operates in its own core business area on the basis that no one player can economically operate and compete in all the sectors. An alternative business model used where a handset subsidy is illegal is to offer an attractive call package to offset the high consumer.

With respect to the supply of cellular infrastructure, there are similarities between the commercial carrier model and the public safety business model. In order to compete, the manufacturer may make a strategic decision to reduce the equipment selling price nearer to cost in response to pressure from the major operator groups for volume. In this case, infrastructure equipment, particularly basestations, will be supplied at a minimum specified feature level for initial rollout. However, the low margin on infrastructure equipment is compensated by increasing the margin on future upgrades, such as software for new features, channel cards for capacity upgrades, and so forth.

The current public safety market is conventionally a single major procurement of voice terminals and infrastructure with maintenance contracts used to structure long-term relationships between customer and supplier. Addition of software-based systems, such as control room systems and the installation of data terminals, may provide opportunities to compete portions of a system outside the original vendor contract. Nevertheless, the degree of sophistication may not be available to all authorities due to cost issues.

SDR now offers the flexibility for the public safety equipment supplier and customer to benefit from business models akin to the cellular business model. A supplier may be able to address sales to smaller authorities with a low capital expenditure budget for new equipment by

selling SDR equipment at a minimum capability level at a lower margin. The supplier can then sell higher margin software upgrades for both radio and operating features either as initial procurements or as part of an annual maintenance package, which can then come from operating expenditure budgets. This business model has other benefits in that the smaller authority can purchase equipment capable of inter-working with the larger authorities by installing features on a single-use basis for a particular incident (if necessary on a "pay-as-you-go" approach—an option that needs to be discussed in the future) along the lines of the cellular industry.

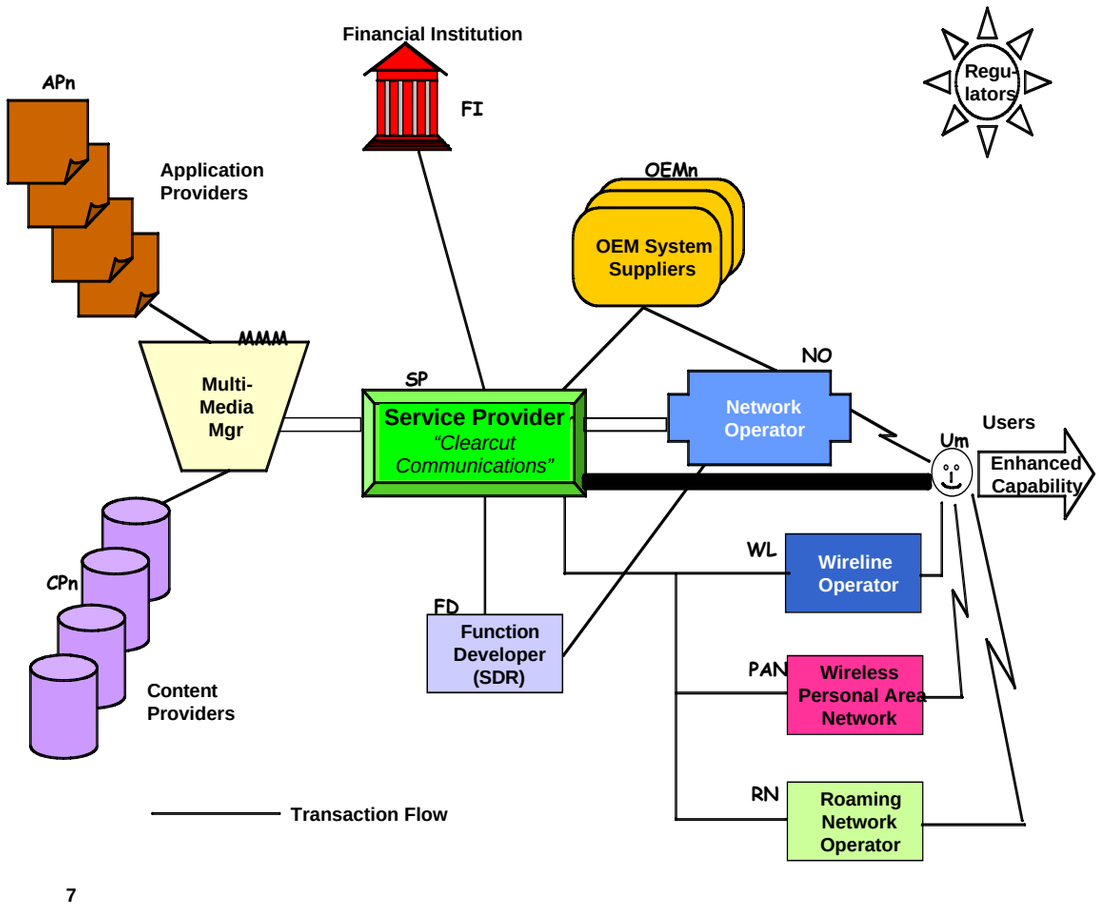

Figure B-2
Commercial Cellular Business Model

C. CONTRIBUTORS TO THIS REPORT

Throughout this report, we have noted discussions within the Public Safety SIG that led to the conclusions and recommendations of this report. Representatives of the following companies and organizations were part of those discussions:

Air Force Research Laboratory Information Directorate
Booz Allen Hamilton (sponsored by U.S. DHS Project SAFECOM)
DataSoft
France Telecom
HYPRES
Jim Gunn
L-3 Communications Government Services Inc., (sponsored by U.S. National Institute of Justice CommTech Program)
M/A-COM
Missouri State Highway Patrol
Motorola
National Institute of Justice
National Public Safety Telecommunications Council
Orange County Florida Public Safety Communications
SAIC (sponsored by the U.S. DHS ICTAP program)
SP&T
Syracuse Research Corporation
Thales